ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse176942020.pdf
https://doi.org/10.30534/ijatcse/2020/176942020

Blockchain - Facilitated IoT Built Cleverer Home with Unrestricted Validation Arrangement

N.Satheesh[1], Ganga Rama Koteswara Rao[2], Subrata Chowdhury[3], Kolla Bhanu Prakash[4], Sudhakar Sengan[5]
[1]Professor, Department of Computer Science and Engineering,
St. Martin's Engineering College, Hyderabad, India. nsatheesh1983@gmail.com
[2]Professor, Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India. grkraoganga@gmail.com
[3]School of Computer Science, Vels University VISTAS Pallavaram,
Chennai, Tamil Nadu, India. subrata895@gmail.com
[4]Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, A.P, India. drkbp@kluniversity.in
[5]Sree Sakthi Engineering College, Coimbatore, Tamil Nadu, India. sudhasengan@gmail.com

ABSTRACT

The growing blockchain technology proves promising opportunities for enhancing the industrialized system and the Internet of Things (IoT) by given that idleness, storage space, and encryption for applications. Over the last few years, many new applications have started to emerge in industrial IoT, and blockchain technologies have attracted the attention of many researchers in academic and industrial. Decentralized security and privacy system based in Blockchain provide an enormous lift to the infrastructure of the IoT. In a smart home, Blockchain technology serves as the perfect gatekeeper for all communication packages. Authentication of identity is required before the terminal accesses the service to prevent access to unauthorized. The fact that trustworthy third parties are introduced destroys not only the independence and flexibility of the IoT system but also source problems such as a breakdown position and unilateral control dangers. A dynamic trust-right method was developed to advance the blockchain output and decrease the no. of authenticated communication in new blocks. A review and verification solutions based on the blockchain technology of the state of the art identity organizations. This article describes a decentralized model of identity verification that can guarantee autonomy and security initiative.

Key words: Internet of Things, Smart Home System, Blockchain, Security, Privacy.

1. INTRODUCTION

The Internet of Things (IoT) [1] becomes a new technology that significantly increases research topics and opens up new marketing efforts for industrial and social IoT platforms. In the last few years, in many fields, like economics services, health care, etc., the use of IoT solutions in industrial enterprises increased [2]. The IoT is a smart system of integrated electronic devices, cars, home appliances, and thousands of sensors and actuators. Authentication as a process of determining whether someone or something is who or what it is declaring to be is the key component of any trustworthy on-line system which handles sensitive data or transactions [3]. IoT exchanges large quantities of critical information and information concerning privacy and is usually cyber-assailed. IoT devices have low-weight economic components that do not have any costly additional safety implications for energy consumption and overhead processing [4]. For the implementation of the IoT, BC provides efficient decentralized privacy and security approaches. The IoT device is the key to security using the above analysis [5][6]. Most IoT terminals usually use password authentication to prevent unauthorized access to the network of the system.

1.1. Blockchain Authentication

The unchanging blockchain directory needs to check and ensures that users, transactions, and messages are legitimate—authentication of the Blockchain done by smart and Blockchain contracts [7]. An intelligent service agreement generator can be programmed via a reference implementation authentication layer for activating and executing an authentication whenever parties require and self-rule within a defined range of actions [8]. A third party was eliminated to authenticate transactions. Costs can be reduced, and privacy and safety considerably improved. The effort to remove authentication from the distributed environment would be much more effective [9].

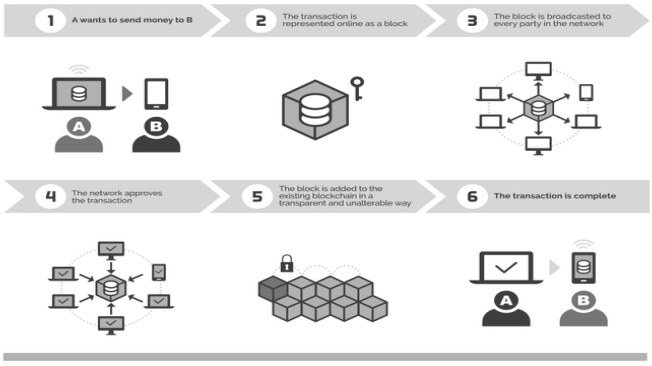

Figure 1: Process of Blockchain

1.2 Blockchain Platform

The evolving blockchain tools proved the excellent potential for the 4th business revolution, which could have a remarkable crash in all sectors of the financial system and change it further during top-notch efficiency [10]. The Blockchain showed

significant possible for solving IoT interoperability. IDC states that up to 20% of IoT build-up provides blockchain service, with over 10% of the world's GDP re-allocated to blockchain-enabled systems by 2030 [11]. Blockchain complements IoT technologies are as follows:

• The decentralized blockchain technology environment plays a crucial role in IoT in communicating between two non-authenticated devices in order to inform devices about their interactions, status, and application programming interfaces [12].

• Blockchain can considerably reduce customer risks and save process improvement costs [13].

• The IoT blockchain should be designed for applications involving transaction and interaction, including smart contracts [14].

Figure 2: A chain of blocks that refers to the previous block in each node.

The smart home workers usually matched the instructions of the owner. If the home security system has a critical power or network failure, the remote owner cannot monitor the system carefully [15]. In such cases, the intruders can, in a short time, cause enormous and unnoticeable losses for the user. Also, burglary attempts in vacant homes and nearby homes can be high chances here. These figures show the need for a community-based interactive home-level system to demote antisocial actions. This study provides a comprehensive model for supporting the confined community of homeowners and for instructions to the owners. The model proposed helps to predict intrusions in the vicinity effectively. The paper focused on the following significant contributions as follows [16]:

- Reduce Data communication and verification cost
- Automatic execution of smart home devices
- Flexible user behavior

2. RELATED WORKS

One fixed login is a typical cross-domain problem report and is made to enable users to a single login, federated identity administration, to access data or services from different application systems. The Application System sends a request for user authentication to the trusted third party by saving the user's identity in a trusted third party when the user has access to the IoT system[17][18][19]. Once the third party ends the authentication, the check code is returned to the IoT system, and the user uses the authentication code to access the application system. A one-sign solution is OAuth. Instead of suggesting an actual authentication algorithm, OAuth implements the proxy authentication of cross-domain identity.

A distributed database that prevents the continuous recording of network transactions can be classified as BC [20] [21]. The BC distributed and applied to a peer-to-peer network. Every BC-connected network node maintains a complete copy of the leader. These ledgers are updated regularly when each transaction is validated. A wearable device, smartphone, and cloud server authentication mechanism. Smartphone manufacturers and wearable devices provide complimentary cloud information [22]. The sensed data are transferred to the cloud to save wearable devices and Smart Phone. Symmetrical key encryption used in the mechanism invented. The most potent problem is that all the symmetrical keys processed on a central server permit the method to fail.

A lightweight authentication system that does not need a central server processing of the secret keys [23]. The problem the researcher identifies in this article is that authentication information stored on a secure server under the existing scheme. The technique proposed is based on physical functions that are unclonable, physical, and are practically impossible to impersonate, related to the physical characteristics of the devices. The major issue is that at least 5 private message certificates are available with new technology and business.[24][25]. In regards, you have to be traded in the server node that probably fails at some point with puf-based authentication data.

The investigator proposed the efficient Blockchain Technology Cross-domain Authentication Scheme and developed the trust model, and system architecture of Blockchain's Certification Agency[26] The BCCA Trust model is based on the Blockchain root CA that connects the consortium chain and the certificate hash value registered for secure and effective cross-domain authentication. In order to reinforce trust and transfer, Chen et al. proposed a trust transfer system based in Blockchain. The unified trust service problem at the national level has been resolved through an agreement in this solution. Specific CA[27] management functions were transferred to the Blockchain, and all security areas integrated into a private consortium had root CA. Trustroam is a roaming authentication scheme distributed to Blockchain. Contrary to the previous two systems, Trustroam checks trigger a smart contract, and every check is a transaction and not a database, which uses Blockchain to request data from the Blockchain during the verification process. A multi-heterogeneous Blockchain Domain Authentication System consists of an IBC Domain Blockchain Proxy Server, and a Blockchain Domain Certification Server in the PKI domain was suggested by the author. The communication between IBC and PKI is safe and efficient[28][29].

The newly developed BC paradigm's design rules depict the common security problems of SDN [30][31] in IoT clouds and argue that BC is a key element of safety for solutions involving SDN and IoT. Software-defined networking offers efficient, interconnected cloud infrastructure with dynamic network reconfiguration. The study explores the potential for using BC, and a distributed data structure used to create a digital deal record and a possible past record of transactions. This finding permits data transmission, independent of the network size and geographic distribution, encrypted between linked nodes.

Using cloud-based trusted services, the confidentiality, integrity, and authenticity of data and communication is ensured by the necessary trust levels and provides the ideal solutions [32][33]. PKI's team with TTP offers technically sound and lawful

methods for secure authentication and authorization. PKI is a public key cryptography means of authentication [39]. It allows users to authenticate the other party without shared secret information based on a certificate. Single-Sign-On is an example of cloud TTP authentication. When a user gets site authentication, he can access other websites with a statement, and he/she does not need to be authenticated. But there are bottlenecks in the security and intolerance of the system that the specific third party exists as an authentication server or certification authority [34].

The IoT platform plays a vital role in IoT systems, providing smart, connecting resources, and enabling IoT to connect, analyze large datasets, and develop apps. The IoT platform is required to address the above challenges by (a) asset visibility; (b) technology integration; and (c) cybersecurity [37][38]. To address these challenges, IoT can also have a significant impact on the behavior, either by customers or users. Most existing industrial plants like microgrids, IoT smart grids, ad-hoc vehicle networks cannot connect to IoT with built-in intelligence that requires IoT interfaces. On the other hand, new technologies like the enhanced reality support operators in IoT, which can improve the interaction and predictive behaviors of the process and therefore simplify and improve efficiency [35][36].

3. PROPOSED METHODOLOGY

The gated viewpoint of the community shares responsibilities between the associated levels of the home and helps others to track and report on the overlay or prediction of an entirely failed state of a member of the community. The smart home miner typically concentrates on owner interactions. This study offers an interacting model to identify unexpected and improper events with trusted external miners [40][41]. It helps predict the intrusion attempts nearby and inform local authorities in a split second. This work aims mainly at presenting a distributed authentication and authorized BC method for communication between devices in different systems. Communication between devices of a similar system of different systems can be made.

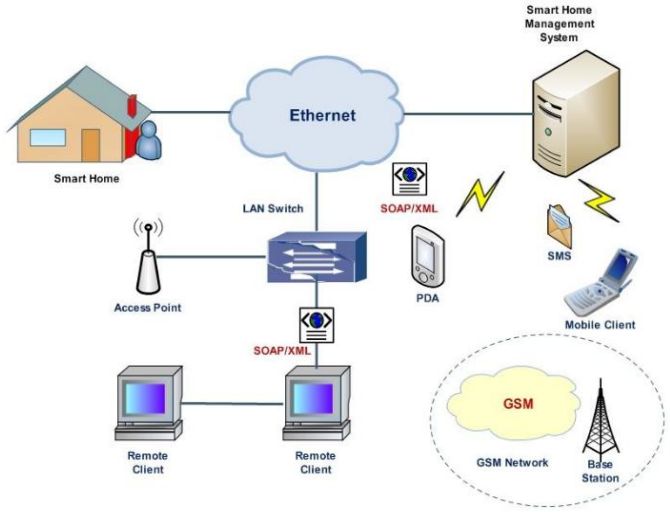

Figure 3: The architecture model for Blockchain and IoT for smart home system

3.1. The Block

A block is referring to files where data about the blockchain network is permanently stored [42]. A block is like pages of a ledger or an account book. Each time a block is completed, it gives way to another block [43]. Data stored in blocks cannot be altered. The genesis block, genesis. Json is the first block of a blockchain.

3.2. Hashing

Each layer consists of transaction history and hashed Blockchain. A hash function takes the input value and produces a probabilistic output value for the input value. Each input has a specific output. The application process of the Hash feature to each data is called Hash, and the output is called the Hash value or the Hash [44]. A key feature of a safe hash function is that it is just one way. Hashing means that, because of the Hash, what the input was cannot be determined. Hashing with Blockchains is widely used. For instance, a hacking process of public keys takes Blockchain addresses. Cryptocurrency transactions computed using keccak-256 to have a public key [45].

3.3 Blockchain

A blockchain is a valid transaction blockchain—each block hash to the initial block in the Blockchain [46]. The system uses a peer-to-peer network, which proves that the network links every server. After authenticating the transaction, it is broadcast to the network and added to every blockchain copy.

3.4. Transaction Structure

There are five parameters of a single community alert transaction, such as Previous Transaction, transaction number, Target Device IDs, transaction type, and Community ID, as shown in Table 1.

Table 1: Transaction Structure

Earlier Transaction	Transaction ID	Device ID	Transaction Type	Resultant Multi-Sign Transaction	The Public ID
N = Origin T	10101	A001	Origin : 0 Access: 1 Store:2 Monitor :3	Keep Sign of Request	ID_1 to ID_n

4. ARCHITECTURE DESIGN OF BLOCKCHAIN-ENABLED IOT

Blockchain nodes can generally be classified as (a) Full Weight Node, (b) Light Weight Node:

(a) Full Weight Node [47]: All blocks and transactions can be accessed. FWN can act as a mining node, which generates Blockchain blocks.

(b) Light Weight Node [48]: Only part of blockchain data can be protected and delivered by LWN because of limited resources. The solution enables lightweight, intelligent devices to be an LWN, offering new transactions spread between nodes and eventually added to a Blockchain block.

4.1. System Architecture

The Blockchain allows IoT systems to distribute and verifiably connect untrusted devices. Figure 4 shows an architecture for blockchain-enabled IoT systems, which includes the two essential [49][50] elements:
a) Networks of IoT resources
b) Blockchain network, whether the records on the decentralized private network all information in systems
c) Management hub, focusing mainly on system management and maintenance.
d) Key servers for authentication and data encryption of the necessary cryptographic keys.
e) The users who request access to IoT resources are the customers.
f) An intelligent contract provides system interfaces between IoT and blockchain components.

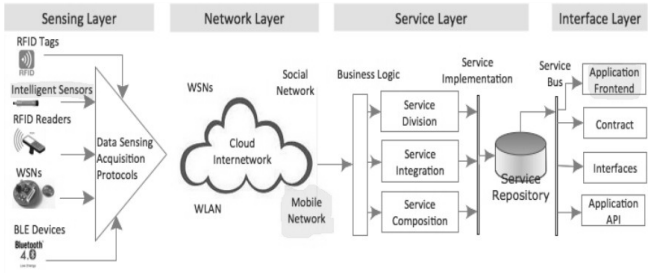

Figure 4: The proposed architecture of Smart IoT platform

4.2. IoT enabled Blockchain security and privacy

In the evolving IoT ecosystem, safety incidents and vulnerabilities are expanding. IoT has significantly expanded the security attack surface due to its exclusively scale and inextricable interconnection, and a lot needs to be done from tool authentication to proper authentication for new smart contract generation. In particular, intelligent contract security and privacy research is an up-and-coming area. The following features in implementing security solutions must take into consideration: (a) the identity and access management of digital primers; (b) the dynamic and continuous evolution of IIoT entities; (c) the uncertain design of IIoT infrastructure, devices, and users, and privacy.

5. Data and algorithms structures

5.1. Local Blockchain

A private local BC monitors transactions. The transaction life cycle begins with evolution. Each block of the local BC contains two-block headers. The policy headers are lean towards the authorization and access control part of the system when the headers in blocks guarantee the immutable property of the Hash. 4 A policy header provides parameters as Requester ID, Action Type, Device ID, and Action.

5.2. Community Blockchain

A private BC tracks the alert transactions of the communities. Three parameters include the Request ID, Request Community ID, and Alert information—the simple form of the community alert system block chain algorithm.

5.3. Community Blockchain Algorithm

Figures 5 and 6 demonstrate the simplified form of the Community Alert System BC algorithm. SHA256 is used to encrypt the requester's signature. Transaction details and the encryption and add-on BC provided for the Append Blocks. The certificate authority blocking method proves its work, but if necessary, trusted people in the community.

```
require 'digest/sha1'
class CommunityBlockChain
  DEGREE=6
  def initialize(details)
    @@blocks = []
    append_blocks(details)
  end
  def chain(details)
    preceder = @@blocks.last
    append_blocks(details, preceder[:signature])
  end
  def verify_blocks
    blocks = @@blocks.last[DEGREE]
    for i in 1 to (blocks.size-1)
      signature = encrypt(create_record(blocks[i][:time], |
            blocks[i][:content], blocks[i-1][:signature])
      return false if signature!= blocks[i][:signature]
    end
  end
  private
  def append_blocks(details,signature='')
    block = create_block(details, signature)
    block[:signature] = encrypt(block)
    @@blocks << block
  end
  def create_block(content, signature='', time=Time.now())
    {
       :content => details,
       :signature => signature,
       :time =>time
    }
  end
  def encriypt(block)
     Digest::SHA256.hexdigest(block.to_json )
  end
end
```

Figure 5: Community Blockchain Algorithm

6. RESULT AND DISCUSSION

We created an experimental environment, as shown in Figure 6, to evaluate the performance of the proposed Blockchain IoT system. There are 10 PC servers with the proposed system in this experimental environment. A security domain authentication server is displayed on each server. The authentication server is responsible for the permission of cross-domain access and for device-cross-domain access authentification. These ten servers are a Blockchain consortium. In every security domain, we also deploy an IoT device with client authentication software installed.

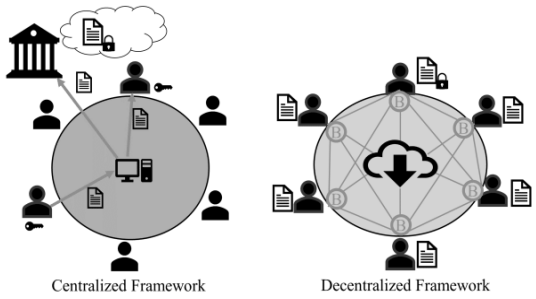

Figure 6: Blockchain IoT System

The current research describes multi-domain access links between 5 and 10 security domains in turn and metrics the change in the simulations of authenticated certificates as domains increase. First of all, for illustration, we access new security domains, then we have key security domains, etc. and finally, we expand to ten security domains. The outcome of the research is included in Figure 7. We found from this diagram that the processing time of the authority does not exceed 8 ms, and in most trials, it does not exceed 4 *ms*.

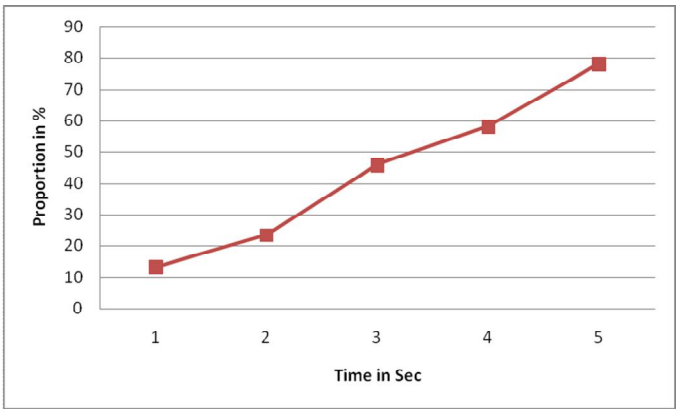

Figure 7: Distribution of execution time for different thresholds

Table 2: Server Execution Time

Authentication Server (*T*)	Time in Sec
10	13.16
20	23.34
30	45.89
40	58.19

The discovery of this new mechanism creates a secure platform for service providers to authenticate users with no single point of failure and prevent attacks and leakages of user data. This solution is a perfect reference point for verification of personal information without exposing the information to a service provider. Blockchain identity management and authentication solution by design distributed, decentralized, and fault-tolerant, which decreases the deployment and maintenance cost. However, scalability seems to be the biggest challenge with public Blockchain. Some argued that by centralizing some parts of the technology, blockchain identity management would be more cost-effective and secure. And On the other hand, blockchain technology-as-a-Service enables clients to leverage cloud-based solutions to build, host, and provide their apps and smart blockchain agreements.

6.1. Review of results

In order to validate the effectiveness of the Blockchain-IoT method when the full load changes, we have tested network data with 50 nodes. The experiment adjusted network performance over a period other than fixed network per sec of the conventional BC transactions: the transaction count is adjusted to 10, 20, 30, 40, and 50. In the experiment, the outcomes are shown (figure 8).

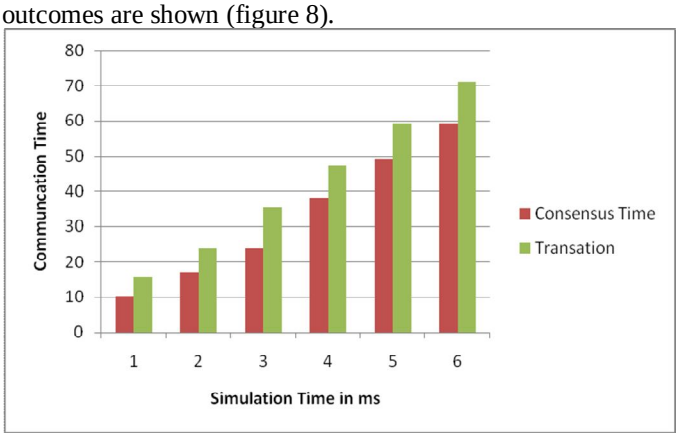

Figure 8: Dynamic regulation of blockchain utilization efficiency

5. CONCLUSION AND FUTURE WORK

In order to form, collect, process, transmit and store data together, different systems are integrated into a sophisticated IoT platform. Industries actively want to block the IoT industry's processes. We have made innovations in traditional authentication, including a multi-domain authorization system based on the cryptography threshold and smart home devices for cross-domain authentication. A blockchain-enabled IoT framework introduced, discussing essential methodologies. Fundamental problems and requirements are discussed. We also examined the investigation challenges and trends in Blockchain-enabled Smart Home IoT devices. Results from experiments show that Blockchain IoT is suited for many IoT scenarios and provides excellent processing performance and flexibility.

In the future, it will be further explored to develop its application domains and perform a quantitative investigation on their performance through the blockchain implementation mechanism between RCL, REL, and the data center-computers.

REFERENCES

[1] Alizadeh Mojtaba, A.S., Zamani Mazdak, Baharun Sabariah, Sakurai Kouichi, **Authentication in mobile cloud computing: A survey**, *Journal of Network and Computer Applications*, 2016. 61: p. 59-80.

[2] M. Yli-Ojanper, S. Sierla, N. Papakonstantinou, and V. Vyatkin, **Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study**, *Journal of Industrial Information Integration*, 2018.

[3] Shu Yun Lim, M.L.M.K., Tan Fong Ang, **Security Issues and Future Challenges of Cloud Service Authentication**, *Acta Polytechnica Hungarica*, 2017.

[4] Ghazizadeh E., M., J. L. A., Zamani, M., Pashang, A. **A survey on security issues of federated identity in the cloud computing. in Cloud Computing Technology and Science (CloudCom)**, *IEEE 4th International Conference on.* 2012.

[5] M I Awang, M.A.M., R R Mohamed, A Ahmad, N A Rawi, **A Pattern-Based Password Authentication Scheme for Minimizing Shoulder Surfing Attack. International Journal on Advanced Science**, *Engineering and Information Technology*, 2017.

[6] Miglani, A., Kumar, N., Chamola, V., Zeadally, S. **Blockchain for Internet of Energy management: Review, solutions, and challenges.** *Comput. Commun.* 2020,

[7] Damiano, D.; Francesco, M.; Paolo, M. **Blockchain 3.0 applications survey**, *J. Parallel Distrib. Comput*. 2020, 138, 99–114.

[8] Wang, X.; Yang, L.T.; Wang, Y.; Ren, L.; Wang, Y.H. ADTT: **A Highly-Efficient Distributed Tensor-Train Decomposition Method for IIoT Big Data**. *IEEE Trans. Ind. Inform.* 2020.

[9] Wang, B.; Kong, W.; Guan, H.; Xiong, N.N. **Air Quality Forecasting Based on Gated Recurrent Long Short Term Memory Model in Internet of Things**. *IEEE Access* 2019,

[10] El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. **A survey of internet of things (IoT) authentication schemes**, *Sensors (Switz.)* 2019, 19, 1141.

[11] S. Mumtaz and A. Al-Dulaimi and V. Frascolla and S. A. Hassan and O. A. Dobre, **Guest Editorial Special Issue on 5G and Beyond Mobile Technologies and Applications for IoT**, *IEEE Internet of Things Journal*, Vol. 6, No. 1, pp. 203–206, 2019.

[12] L. Urquhart and D. McAuley, **Avoiding the internet of insecure industrial thing**s, *Computer Law & Security Review*, vol. 34, no. 3, pp. 450 – 466, 2018.

[13] Ismail, M., Prakash, K. B., & Rao, M. N. (2018). **Collaborative filtering-based recommendation of on-line social voting**. *International Journal of Engineering and Technology (UAE)*, 7(3), 1504-1507. DOI:10.14419/ijet.v7i3.11630

[14] Prakash, K. B. (2017). **Content extraction studies using total distance algorithm**. Paper presented at the Proceedings of the 2016 2nd *International Conference on Applied and Theoretical Computing and Communication Technology*, iCATccT 2016, 673-679. DOI:10.1109/ICATCCT.2016.7912085

[15] Prakash, K. B., Rajaraman, A., & Lakshmi, M. (2017). **Complexities in developing multilingual on-line courses in the indian context**. Paper presented at the Proceedings of the 2017 *International Conference on Big Data Analytics and Computational Intelligence, ICBDACI 2017*, 339-342. DOI:10.1109/ICBDACI.2017.8070860.

[16] Sengan, Sudhakar, Arokia Jesu Prabhu, L., Ramachandran, V., Priya, V., Ravi, Logesh, Subramaniyaswamy, V., **Images super-resolution by optimal deep AlexNet architecture for medical application: A novel DOCALN**, *Journal of Intelligent & Fuzzy Systems*, pp. 1-14, 2020, DOI: 10.3233/JIFS-189146.

[17] V Vijaya Kumar, M Devi, P Vishnu Raja, P Kanmani, V Priya, Sengan Sudhakar, Krishnamoorthy Sujatha, **Design of peer-to-peer protocol with sensible and secure IoT communication for future internet architecture**, *Microprocessors and Microsystems*, Vol.78, 2020, 103216, https://doi.org/10.1016/j.micpro.2020.103216.

[18] Vijaya Kumar Veerabathiran, Devi Mani, Sangeetha Kuppusamy, Balu Subramaniam, Priya Velayutham, Sudhakar Sengan & Sujatha Krishnamoorthy, **Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption**, *Soft Computing*, 2020, DOI 10.1007/s00500-020-05119-9.

[19] M. Karthikeyan, K. Sharmilee, P.M. Balasubramaniam, N.B. Prakash, M. Rajesh Babu, V. Subramaniyaswamy, Sudhakar Sengan, **Design and Implementation of ANN-based SAPF Approach for Current Harmonics Mitigation in Industrial Power Systems**, DOI 10.1016/j.micpro.2020.103194, *Microprocessors, and Microsystems* (2020).

[20] Sudhakar Sengan, Subramaniyaswamy, V., Sreekumar Krishnan Nair, Indragandhi, V., Manikandan, J., Logesh Ravi, **Enhancing cyber-physical systems with hybrid smart city cybersecurity architecture for the secure public data-smart network**, DOI 10.1016/j.future.2020.06.028, *Future Generation Computer Systems* (2020).

[21] Ganesh Kumar, K and Sudhakar Sengan, **Improved Network Traffic by Attacking Denial of Service to Protect Resource Using Z-Test Based 4-Tier Geomark Traceback (Z4TGT).** *Wireless Personal Communications* (2020), DOI 10.1007/s11277-020-07546-1.

[22] E.Punarselvam, Mohamed Yacin Sikkandar, Mohsen Bakouri, N.B.Prakash, T. Jayasankar, S.Sudhakar, **Different loading condition and angle measurement of human lumbar spine MRI image using ANSYS**, Springer, *Journal of Ambient Intelligence and Humanized Computing*, DOI 10.1007/s12652-020-01939-7,11, 2020.

[23] R.Vasanthi, R.Jayavadivel, K.Prasadh, J.Vellingiri, G.Akil arasu, S.Sudhakar, P.M.Balasubramaniam, **A novel user interaction middleware component system for ubiquitous soft computing environment by using fuzzy agent computing system**, Springer, *Journal of Ambient Intelligence and Humanized Computing* (2020), DOI 10.1007/s12652-020-01893-4.

[24] S.Sudhakar, V.Vijayakumar, C.SathiyaKumar, V.Priya, Logesh Ravi, V.Subramaniyaswamy, **Unmanned Aerial Vehicle (UAV) based Forest Fire Detection and monitoring for reducing false alarms in forest-fires**, Elsevier-*Computer Communications* 149 (2020) 1–16, DOI 10.1016/j.comcom.2019.10.007.

[25] Sudhakar Sengan & Chenthur Pandian S, 2016, **Hybrid Cluster-based Geographical Routing Protocol to Mitigate Malicious Nodes in Mobile Ad Hoc Network**, InderScience-*International Journal of Ad Hoc and Ubiquitous Computing*, Vol.21, No.4, pp:224-236.

[26] Avuthu Sai Meghana, Sudhakar S, Arumugam G, Srinivasan P, Kolla Bhanu Prakash, **Age and Gender prediction using Convolution, ResNet50, and Inception ResNetV2**, *International Journal of Advanced Trends in*

Computer Science and Engineering, Vol. 9, No.2, March–April 2020, pp: 1328-1334 https://doi.org/10.30534/ijatcse/2020/65922020.

[27] Yellapragada SS Bharadwaj, Rajaram P, Sriram V.P, Sudhakar S, Kolla Bhanu Prakash, **Effective Handwritten Digit Recognition using Deep Convolution Neural Network**, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 9, No.2,2020,pp:1335-1339,https://doi.org/10.30534/ijatcse/2020/66922020.

[28] Donepudi Babitha, Jayasankar.T, Sriram V.P, Sudhakar S, Kolla Bhanu Prakash, **Speech Emotion Recognition using State-of-Art Learning Algorithms**, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol.9, No.2, March–April 2020, PP:1340-1345, https://doi.org/10.30534/ijatcse/2020/67922020.

[29] Murugan G, Syed Musthafa A, Abdul Jaleel D, Sathiya Kumar C, Sudhakar S, **Tourist Spot Proposal System Using Text Mining**, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol.9, No.2, March–April 2020, pp: 1358–1364, https://doi.org/10.30534/ijatcse/2020/70922020.

[30] Murugan G, N.Keerthana, Sujatha Krishnamoorthy, Sudhakar Sengan, Amarendra K, Malladi Srinivas, **Towards Taxonomy for Cloud Computing as Business Models and Deployment: A Technical Review**, *International Journal of Advanced Science and Technology*, Vol. 29, No. 03, (2020), pp. 9096 – 9106.

[31] A.Pushpalatha, D.Prabha, S.Sudhakar, V.P.Sriram, P.Kevin Mario Gerard, S.Sanjay, **A Study Of Detecting Malicious URL Using Convnet**, *International Journal of Scientific & Technology Research*, Vol.9, No.4, April 2020.

[32] Kanmani P, Priya V, Yuvaraj N, Sudhakar S, Sriram V P, **Inaccuracy Correction Method for Moving Shapes and Shadows in Video Coding Object**, *International Journal of Scientific & Technology Research*, Vol.9, No.3, March 2020, PP: 4561-4566.

[33] Jagadeesh Gopal, Vellingiri J, Gitanjali J, Arivuselvan K, Sudhakar S, **An Improved Trusted On-Demand Multicast Routing with QoS for Wireless Networks**, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol.9, No.1, January–February 2020, pp.261-265, https://doi.org/10.30534/ijatcse/2020/39912020.

[34] R.Gowthamani, K.Sasi Kala Rani, E.Mohanraj, S.Sudhakar, **Enhancing Security Through Blockchain Technology –A Quick Review**, *International Journal of Scientific & Technology Research*, Vol.9, No.2, February 2020, pp: 5126-5129.

[35] S.Biruntha, S.Balaji, S.Dhyakesh, B.R.Karthik Srini, J.Boopala, S.Sudhakar, **Digital Approach For Siddha Pulse Diagnosis**, *International Journal of Scientific & Technology Research*, Vol.9, No.2, February 2020, pp: 2140-2143.

[36] P.Deivendran, K.Anbazhagan, P.Sailaja, E.Sujatha, M.Rajesh Babu, S.Sudhakar, **Scalability Service In Data Center Persistent Storage Allocation Using Virtual Machines**, *International Journal of Scientific & Technology Research*, Vol.9, No.2, 2020, pp: 2135-2139.

[37] K.Devipriya, D.Prabha, V.Pirya, S.Sudhakar, **Deep Learning Sentiment Analysis For Recommendations In Social Applications**, *International Journal of Scientific & Technology Research*, Vol.9, No.01,2020, pp: 3812-3815.

[38] K.Sasi Kala Rani, D.Ramya, J.Manikandan, S.Sudhakar, **Monitoring Emotions In The Classroom Using Machine Learning**, *International Journal of Scientific & Technology Research*, Vol.9, No. 01,2020, pp:3723-3726.

[39] P.M.Balasubramaniam, S.Sudhakar, Sujatha Krishnamoorthy, V.P.Sriram, S.Dhanaraj, V.Subramaniyaswamy, *Investigations, and Strategy of Intelligent Controller (ACBIC) for DC-Link control in SAPF system for Industrial power systems a control strategy*, *Journal of Discrete Mathematical Sciences & Cryptography*, (2020) https://doi.org/10.1080/09720529.2019.1668145.

[40] P.M.Balasubramaniam, S.Sudhakar, Sujatha Krishnamoorthy, V.P.Sriram, S.Dhanaraj, V.Subramaniyaswamy, T.Rajesh, **An efficient control strategy of shunt active power filter for asymmetrical load condition using time-domain approach**, *Journal of Discrete Mathematical Sciences & Cryptography*, 2020, https://doi.org/10.1080/09720529.2019.1668136.

[41] Satheesh N, Sudha D, Suganthi D, Sudhakar S, Dhanaraj S, Sriram VP, Priya V, **Certain improvements to Location aided packet marking and DDoS attacks in internet**, *Journal of Engineering Science and Technology*, Vol. 15, No. 1 (2020), pp: 94-107.

[42] Sathiya Kumar.C, Priya.V, Sriram.V.P, Sankar Ganesh.K, Murugan.G, Devi Mani, Sudhakar.S, **An Efficient Algorithm for Quantum Key distribution with Secure Communication**, *Journal of Engineering Science and Technology*, Vol. 15, No. 1 (2020), pp:77-93.

[43] S.Sudhakar, N.Satheesh, S.Balu, Amireddy Srinish Reddy, G.Murugan, 2019, **Optimizing Joins in a Map-Reduce for Data Storage and Retrieval Performance Analysis of Query Processing in HDFS for Big Data,** *International Journal of Advanced Trends in Computer Science and Engineering, (IJATCSE)*, Vol.8, No 5, pp: 2062-2067, DOI: 10.30534/ijatcse/2019/33852019.

[44] Sudhakar Sengan, Chenthur Pandian S, 2015, **Investigation of Attribute Aided Data Aggregation Over Dynamic Routing In Wireless Sensor**, *Journal of Engineering Science and Technology, School of Engineering*, Taylor's University, Vol. 10, No.11 (2015) 1465 – 1476.

[45] A.U.Priyadarshni and S.Sudhakar, 2015, **Cluster-Based Certificate Revocation by Cluster Head in Mobile Ad-Hoc Network**, *International Journal of Applied Engineering Research*, Vol. 10 No.20, pp:16014-16018.

[46] Sudhakar Sengan and Chenthur Pandian S, 2013, **Trustworthy Position-Based Routing to Mitigate against the Malicious Attacks to Signifies Secured Data Packet using Geographic Routing Protocol in MANET**, *WSEAS Transactions on Communications*, Vol.12, No.11,pp.584-013.

[47] Sudhakar Sengan and Chenthur Pandian S, 2013, **A Trust and Co-Operative Nodes with Affects of Malicious Attacks and Measure the Performance Degradation on Geographic Aided Routing in Mobile Ad Hoc Network**, *Life Science Journal*, Vol. 10, No. 4s, pp. 158-163, 2010.

[48] Sudhakar Sengan and Chenthur Pandian S, 2012, **An Efficient Agent-Based Intrusion Detection System for Detecting Malicious Nodes in MANET Routing**, *International Review on Computers and Software (I.RE.CO.S.)*, Vol. 7, No. 6, pp. 3037-304.

[49] Sudhakar Sengan and Chenthur Pandian S, 2012, **Secure Packet Encryption and Key Exchange System in Mobile Ad hoc Network**, *Journal of Computer Science*, No. 6, pp. 908-912.

[50] Sudhakar Sengan and Chenthur Pandian S, 2012. **Authorized Node Detection and Accuracy in Position-Based Information for MANET**, *European Journal of Scientific Research*, Vol. 70, No. 2, pp. 253-265.