A Detailed Survey on Augmented Data Recognition Towards Automated Shopping With Lifi and IoT

V. Sivasooriya[1*], M. Saroja[2], M. Venkatachalam[2], N. Pradheep[3]
[1]Research Scholar, Department of Electronics, Erode Arts and Science College, Erode-9.
[2]Associate Professor Department of Electronics, Erode Arts and Science College, Erode – 9.
[3]Assistant Professor, Department of Electronic & Communication, Salem Sowdeswari College, Salem-10
*Corresponding author E-mail: [1]riya.vetriselvan@gmail.com

ABSTRACT

The recent development in automated shopping encourages E-Shop and M-Shop. However, the most shopping is performed through personal visit on shops where the customer waits on the queue for long time. The time taken on billing really suffocates the customer due to the existing billing techniques. In general, the billing of any purchase is performed by scanning the barcode attached to the product which claims higher time complexity and increases the queue size. Similarly, there are number of approaches available towards Augmented Data Recognition. This paper presents a detailed review on the methods of augmented data recognition and present a survey on light fidelity (Li-Fi) based communication approaches towards development of wifi communication. Also the paper presents the scenario how the Internet of Things (IoT) has been used for the development automated shopping. Finally, a comparative study on different methods of automated shopping, Li-Fi communication and IoT has been presented.

Keywords: Augmented Data Recognition, Automated Shopping, LI-FI, IOT, QOS, Cloud, Data Security.

1. INTRODUCTION

The growth of information technology has been applied for several domains. The modern society involves shopping frequently by visiting the shopping spots. They spend much time in shopping and selecting the products they required. The number of customers visiting the shop is higher and they form a queue to bill their purchase. However, the time of billing is highly close to the time of selecting the product in most time and even if the customer purchases minimum products then also they have to wait for long time to make their bills. This make them worry about shopping because waiting to make the bills is really huge. Such higher time complexity is introduced by the communication aspects and components being used.

The general billing in shopping units are performed by scanning the barcode attached to the product. The communication to the scanner and the data application is performed through the radio frequency communication which is slower. This increases the time complexity of billing and increases the size of queue. This encourages the requirement of automated shopping systems with high speed communication. This research is about the development of automated shopping and communication development towards QoS (Quality of Shopping). The quality of shopping is depending on various parameters like the time, cost management and communication support. The time complexity represents the time taken for the shopping and billing. The cost management represents how the shopping system support the management of products being purchased. The communication support represents how the automated system performs communication between the billing server, product server and trolley.

On the other side, the quality of shopping has been represented by handling the customer needs. For example, when a customer selects and places the product in the basket, then the customer would not know much about the variant of products and benefits of purchasing such product. So, the shopping system should intimate the customer about other variants of the product by display and should support smart shopping. Towards this, the Li-Fi (light Fidelity) technique based communication has been recommended in this article. The Li-Fi is an another form of wireless communication where the data transmission is performed through light. The entire survey is about the data transmission, and data security in cloud towards QoS.

The quality of shopping can be improved by adapting IoT (Internet of Things) devices. The recent development in communication technology invented IoT which has been used for several purposes. The IoT devices come with sensors, transmitters and receivers. This supports the IoT device to scan the barcode of product and communicate with the data servers and bounce back. The most organizations maintain the data with different distributed servers. The growing size of data encouraged the cloud solutions where there is no restriction for the size and volume of data. The IoT devices are capable of communicating with the cloud servers and billing application to support automated shopping. However, the security of data in cloud and communication should be considered in different factors. The cloud security is performed by using different encryption schemes. The public/private key based approach uses the keys to perform data encryption. Similarly, attribute based encryption (ABE) has been used in several occasions. This paper analyzes different security measures on various data security requirements and presents in detail.

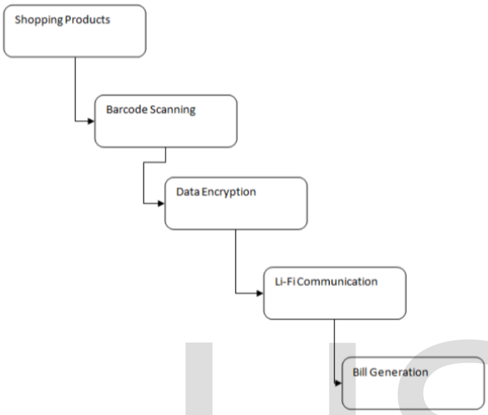

Figure 1: General Working Principle of Automated Shopping

The working principle of Li-Fi based automatic shopping and the detailed stages is presented in this section. First the list of products from the shopping basket are identified. Each product is scanned for their price using the scanner and the code is communicated with the cloud server and its price and variants are obtained. Then the product present in the basket and their details are encrypted using some scheme and transmitted through IoT devices. Finally, the billing is generated at the counter and the customer need not wait for long time.

2. LITERATURE SURVEY

This section discusses various methods of automated shopping, data security, Li-Fi communication approaches and so on.

2.1 AUGMENTATION BASED APPROACHES

In [1], the author presents image augmentation algorithms which include geometric transformations, color space augmentations, kernel filters, mixing images, random erasing, feature space augmentation, adversarial training, generative adversarial networks, neural style transfer, and meta-learning. The application of augmentation methods based on GANs is heavily covered in this survey.

In [2], the author proposes to use a deep convolutional neural network (dCNN) using augmented face dataset to extract discriminative features from face images containing synthetic makeup variations. The augmented dataset containing original face images and those with synthetic make up variations allows dCNN to learn face features in a variety of facial makeup.

Data augmentation techniques have been widely used in visual recognition tasks as it is easy to generate new data by simple and straight forward image transformations. However, when it comes to text data augmentations, it is difficult to find appropriate transformation techniques which also preserve the contextual and grammatical structure of language texts. In this paper, we explore various text data augmentation techniques in text space and word embedding space. We study the effect of various augmented datasets on the efficiency of different deep learning models for relation classification in text [3].

Deep learning is a revolutionary technique in artificial intelligence applications. According to neural networks which are working with high error rates, this technique exceeds the recognition properties of the human brain. Instead of using a pattern, augmented reality applications that use deep learning need to be educated an object which an information shown on it. For example, when the source object is a human hand, recognition can be performed in all of the different positions of any human hand. It is clear that deep learning will be effective in the future of the augmented reality [4].

In [5], the author investigates the capability of a deep convolutional neural network (CNN) combined with three types of data augmentation operations in SAR target recognition in face recognition.

In [6], Augmented Reality (AR) plays major role in current technology. AR is mapping real world environment with computer based virtual environment. This research is a Mobile Application, based on AR. Once user selects a picture of a fruit, the image would be processed and display details lively. The application was developed based on client server Architecture.

In [7], the author discussed augmented reality virtual glasses try-on technology on iOS platform to achieve optimal purchase of online glasses, improving try-on speed of virtual glasses, user senses of reality, and immersion. Face information was collected by the input device-monocular camera. After face detection by SVM classifier, the local face features were extracted by robust SIFT. Combined with SDM, the feature points were iteratively solved to obtain more accurate feature point alignment model.

In paper [8], proposes an architecture for combining the AR interface with IoT for an improved shopping experience. The proposed architecture is distributed and therefore scalable such that any IoT product can be accessed on the spot locally without any server restriction and provide intuitive AR-based visualization and interaction for a flexible product trial in the showroom. The author identifed three key architectural components required to support such a seamless and scalable AR service and experience for IoT-ready products: (1) object-centric data management and visualization, (2) mechanism for accessing, controlling, and interacting with the object, and (3) content exchange interoperability.

In [9], the author explores data augmentation using temporal and speed modifications to healthy speech to simulate dysarthric speech. DNN-HMM based Automatic Speech Recognition (ASR) and Random Forest based classification were used for evaluation of the proposed method. Dysarthric speech, generated synthetically, is classified for severity level using a Random Forest classifier that is trained on actual dysarthric speech.

In [10], the author presents first results of the Austrian project (MANGO) which develops mobile assistance for instant, situated information access via Augmented Reality (AR) functionality to support the user during everyday grocery shopping. Within a modern diet - the functional eating concept - the user is advised which fruits and vegetables to buy according to his individual profile. This specific oxidative stress profile is created through a short in-app survey. Using a built-in image recognition system, the application automatically classifies video captured food using machine learning and computer vision methodology, such as Random Forests classification and multiple color feature spaces. The user can decide to display additional nutrition information along with alternative proposals.

In [11], the author investigates data augmentation for deep neural network acoustic modeling based on label-preserving transformations to deal with data sparsity. Two data augmentation approaches, vocal tract length perturbation (VTLP) and stochastic feature mapping (SFM), are investigated for both deep neural networks (DNNs) and convolutional neural networks (CNNs). In addition, a two-stage data augmentation scheme based on a stacked architecture is proposed to combine VTLP and SFM as complementary approaches.

2.2 METHODS OF DATA SECURITY

The user authentication to secure data of encryption algorithm within cloud computing is proposed. Cloud computing allows users to use browser without application installation and access their data at any computer using browser. This infrastructure guaranteed to secure the information in cloud server. [12]

The several levels of multi-coding levels were developed using more than one method to obtain more confidentiality through DNA encryption. A higher level of confidentiality is given by adding Advanced Encryption Standard (AES) and then loading it into the cloud storage. [13]

The hybrid homomorphic encryption scheme based is on the GM encryption algorithm which is additively (single bit) homomorphic, and RSA algorithm which is multiplicative homomorphic. The hybridization of homomorphic encryption schemes seems to be an effective way to defeat their limitations and to benefit from their resistance against the confidentiality attacks have been discussed in this paper. [14]

The author mentions that the cloud user is facilitated with all the 3 encryption techniques 128, 192 and 256bits to choose and based on the size of the data the encryption process can be done. [15]

The concept of cloud data storage security strategy is capable to overcome the shortcomings of traditional data protection algorithms and improving security using steganography, encryption decryption techniques, compression and splitting technique adoptable to better security for the cloud. A desktop application through which user can share data is developed. This paper enhanced advance security goal for cloud data storage. [16]

A Cipher-text Policy Attribute-Based Encryption for maintaining complex access control over encrypted data is with verifiable customizable authorization. The proposed technique provides data confidentiality to the encrypted data even if the storage server is comprised. Moreover, this method is highly secured against collusion attacks. [17]

The security is a foremost important issue for data in cloud. To look after the data from cloud data storage we store the encrypted data in cloud environment. For encrypting the data, different types of encryption methods like RSA, SHA1, and MD5 are used. Further the measure performance of the different encrypted techniques based on the Key size of each encrypted technique to upload data in to the cloud by providing the best way security to data. [18]

A hybrid encryption scheme to support data sharing in banking cloud is developed. This method uses combination of Attribute-Based Encryption and Byte Rotation Encryption Algorithm. The essence of the work is to build up a straightforward platform that can get protection, integrity, and performance for the data exchange from peer to peer. The proposed framework utilizes symmetric cryptography framework. [19]

An Efficient Key-Aggregate Proxy Re-Encryption for Secure Data scheme which combine a key-aggregate approach and a proxy re-encryption scheme was newly developed by W.Chen. It was shown that the size of re-encryption keys is constant. [20]

An efficient cipher text retrieval technique on a large volume of data is proposed. Initially, an index is generated by Porter stemming. Then the Blowfish algorithm is applied for encryption of files to be outsourced. For authorized access, public key encryption based elliptic curve cryptography (ECC) is used for key generation. When keyword queries are transferred to the cloud, it searches the relevant content associated with the index and retrieves the matching files. Then the Blowfish decryption algorithm is used to get the plain text and was done by S.Mudepalli. [21]

2.3 METHODS OF SECURITY IN IOT SYSTEMS

A routing protocol which embeds the multi-layer parameters into the routing algorithm, thus combining the authentication and routing processes without incurring significant overheads is proposed by P. L. R. Chze. The multi-layer parameters include a unique User-Controllable Identification, users' pre-agreed application(s), and a list of permitted devices, thus saving resources by maintaining smaller routing information. [22]

G. Hatzivasilis proposed SCOTRES-a trust-based system for secure routing in ad-hoc networks which advances the intelligence of network entities by applying five novel metrics. The energy metric considers the resource consumption of each node, imposing similar amount of collaboration, and increasing the lifetime of the network. The topology metric is aware of the nodes' positions and enhances load-balancing. The channel-health metric provides tolerance in periodic malfunctioning due to bad channel conditions and protects the network against jamming attacks. The reputation metric evaluates the cooperation of each participant for a specific network operation, detecting specialized attacks, while the trust metric estimates the overall compliance, safeguarding against combinatorial attacks. Theoretic analysis validates the security properties of the system. [23]

A modified version of the RPL routing protocol by introducing the SISLOF Objective Function ensuring that only nodes that share a suitable key can join the RPL routing table. This will ensure that all IoT network nodes connect in a secure method. SISLOF uses the concept of key pre-distribution proposed by Eschenauer and Gligor in the context of the Internet of Things. They introduce the SISLOF Objective Function and explain the modification it does to the RPL messages (DIO and DAO). [24]

A crowd cloud routing protocol is proposed based on opportunistic computing to improve the data transmission efficiency, reliability, and reduce routing overhead in wireless sensor networks. Based on the analysis of the demand of big data processing in wireless sensor network, the data analysis and processing platform for wireless sensor network are designed based on the combination with the cloud computing. [25]

A QoS Aware Cloud Based Routing Protocol is developed for Security Improvement of Hybrid Wireless Network, which analyze the design issues of sensor networks and present a classification and comparison of routing protocols. [26]

A detailed review on routing in cloud environment and a survey on various routing algorithms that are used for the cloud computing processes, the optimal resource allocation techniques used in cloud computing and its applications in various fields are proposed by Mahalakshmi Jeyabalu, Mohsin Nazir and Deepa Metha. [27,28,29]

The various aspects of IoT systems and challenges are discussed by Kazi MasumSadique. IoT data collected from different sensors, nodes and collectors are transferred to the cloud over the internet. IoT devices are used by consumers, healthcare, businesses as well as by the governments. [30]

A trust aware routing algorithm and the design of SecTrust, a lightweight secure trust-based routing framework to identify and isolate common routing attacks in IoT networks are presented. The proposed framework is based on the successful interactions between the IoT sensor nodes, which effectively is a reflection of their trustworthy behavior. [31]

keeping the IoT systems in trust state is the responsibility of Trust Management Mechanism (TMM). Secure routing is important aspect TMM. Also, an approach for secure routing base on multi-objective simulated annealing is presented by A. E. Basabi, Jingsha He and S. M. Hashemi. [32]

A new secure routing protocol based on RPL referred to as Secure-RPL (SRPL) is presented by Chaithra .S. The main aim of SRPL is to prevent misbehaving nodes from maliciously changing control message values such as the rank of a node that may disturb a network by creating a fake topology. [33]

The Routing protocol is used to achieve secure fault tolerant routing to enhance the performance and minimize the energy consumption. The proposed architecture includes a Blowfish algorithm method for secure data transmission. The performance analysis of Routing protocol is done on the basis of Packet delivery ratio and energy consumption. [34]

A novel blockchain-based contractual routing (BCR) protocol for a network of untrusted IoT devices is developed. In contrast to conventional secure routing protocols in which a central authority (CA) is required to facilitate the identification and authentication of each device, the BCR protocol operates in a distributed manner with no CA. The BCR protocol utilizes smart contracts to discover a route to a destination or data gateway within heterogeneous IoT networks. [35]

3. COMPARATIVE STUDY

The methods on augmentation based recognition, data security in cloud and IoT security has been analyzed and compared in Table 1.

Table 1: Comparative study

Method	Feature Used	Advantages	Disadvantages
Geometric Augmentation Network (GAN)	geometric transformations, color space augmentations, kernel filters, mixing images, random erasing, feature space augmentation,	Higher performance on augmentation search	Higher time complexity.
DCNN	Deep convolution neural network uses augmented faces and discriminative features	Higher accuracy in face recognition	Higher time complexity
SAR-Dcnn	Uses three features of augments of face.	Higher face recognition accuracy	Higher time complexity
SVM-SDN	Uses SIFT features from face to perform recognition	SDN is used for training and classification is performed with SVM.	Higher time complexity and false ratio is higher.
DNN-HMM	Uses temporal features to perform automatic speech recognition.	Recognition accuracy is moderate.	The time complexity is higher and lower false ratio.
Hybrid Homomorphic encryption	Uses homomorphic encryption with RSA.	Provides higher resistance to attacks	The time complexity is higher.
Cipher-text Policy Attribute-Based Encryption	Maintains different policies for various attributes to perform encryption.	Provides higher security on collusion attack.	Higher time complexity
Key-Aggregate Proxy Re-Encryption	Combines key aggregate and proxy re-encryption scheme	Uses same size of key for encryption.	The security performance is less.
Blowfish-ECC	Both algorithms are used for encryption	Security performance is higher	Higher time complexity
ABBR	Attribute based byte rotation encryption scheme is used.	Security performance is higher	Time complexity is higher.
SCOTRES	Uses trust based routing.	Introduces moderate security performance.	higher time complexity.
TMM	Routing is performed using trust state	Introduces higher secure routing performance	Introduces less time complexity.
blockchain-based contractual routing (BCR)	Uses central authority in measuring the trust value.	Introduces higher security performance	The time complexity is less.
SecTrust	Performs secure trust based routing	The secure routing performance is higher	Less false classification ratio.

SRRPL	Performs secure routing according to behavior of nodes	Routing performance is higher and reduces routing attacks	Higher time complexity.

4. RESULTS AND DISCUSSIONS

The performance of methods has been measured under various circumstances and obtained results have been compared and presented in detail.

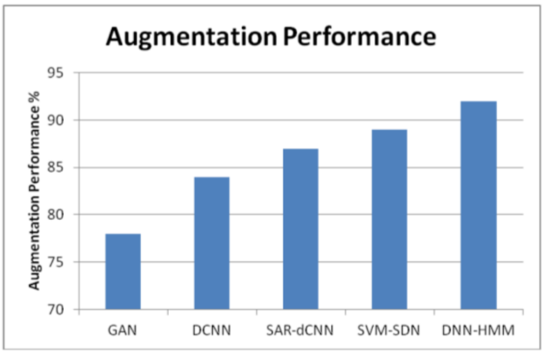

Figure 2: performance on augmentation

The performance on augmentation based automatic shopping has been measured and compared in Figure 2. The performance values has been compared and presented in Figure 2.

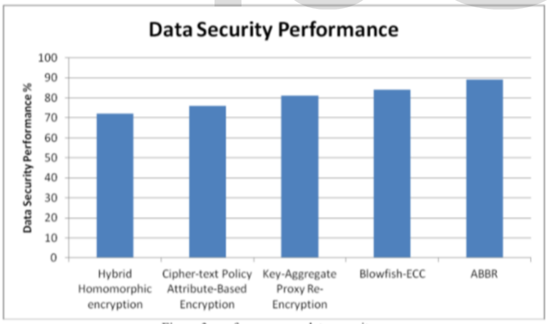

Figure 3: performance on data security

The performance on data security produced by different algorithms have been measured and compared in Figure 3.

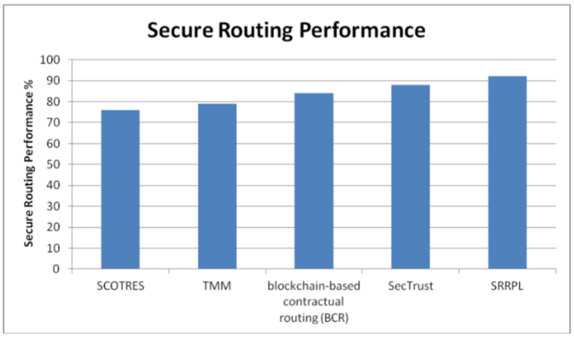

Figure 4: Performance on secure routing

The secure routing performance introduced by different algorithms have been measured and presented in Figure 4.

5. CONCLUSION

This paper discusses various aspects of augmentation based automatic shopping, different methods on feature matching and review based on augmented features. Also, the methods of data security in cloud have been analyzed with different schemes. Further, the routing in IoT systems has been studied. A detailed comparative study on augmentation based recognition, data security in cloud and IoT security has been presented in Table 1. Finally, the performances of different methods on various aspects are presented in Figures. From this review, it is identified that, designing automated shopping solution should consider all the aspects reviewed in this paper

REFERENCES

[1]. Shorten, C., Khoshgoftaar, T.M, (2019) "A survey on Image Data Augmentation for Deep Learning", J Big Data, Vol 6, No. 60 pp. 1-48.

[2]. Mohammed Sajid, et. Al, (2018) "Data Augmentation-Assisted Makeup-Invariant Face Recognition", Hindawi, Vol 01, pp. 1-9.

[3]. Praveen Badimala, (2019) "A Study of Various Text Augmentation Techniques for Relation Classification in Free Text", International Conference on Pattern Recognition Applications and Methods, At Prague, Czech Republic, Vol 01, pp. 360-367.

[4]. Cengiz Gungor, (2017) "A Survey On Augmented Reality Applications Using Deep Learning", Research Gate, pp. 1-13.

[5]. Jung Ding, (2016) "Convolutional Neural Network With Data Augmentation for SAR Target Recognition", IEEE, Geoscience and Remote sensing, vol. 13, issue. 3, pp. 1-5.

[6]. W.A.L.Madushanka, (2014) "Smart Shopping: Building a Tool Based on Augmented Reality, Compusoft", International journal of advanced computer technology, Vol. 3(10), pp. 1186-1192.

[7]. Boping Zhang, (2018) "Augmented reality virtual glasses try-on technology based on iOS platform", EURASIP Journal on Image and Video Processing, volume 01, pp. 1-19.

[8]. Dongsik Jo & Gerard, IoT + AR: pervasive and augmented environments for "Digi-log" shopping experience, Springer, Human-centric Computing and Information Sciences, 2019, pp. 1-17.

[9]. Bhavik Vachchani, (2018) "Data Augmentation Using Healthy Speech for Dysarthric Speech Recognition", Conference on Interspeech, Vol 01, pp. 471-475.

[10]. Georg Waitner, (2018) "MANGO - Mobile Augmented Reality with Functional Eating Guidance and Food Awareness, An Interactive Tool for Speed up the Analysis of UV Images of Stradivari Violin, pp. 425-432.

[11]. Xiaodong Cui ; Vaibhava Goel ; Brian Kingsbury, (2015) "Data Augmentation for Deep Neural Network Acoustic Modeling", IEEE/ACM Transactions on Audio, Speech, and Language Processing, Vol. 23, Iss. 9, Sept, pp. 5582-5585.

[12]. N. Surv, (2015) "Framework for client side AES encryption technique in cloud computing," IEEE (IACC), pp. 525-528.

[13]. N. Mohammed and N. Ibrahim, (2019) "Implementation of New Secure Encryption Technique for Cloud Computing," IEEE (ICCISTA), pp. 1-5.

[14]. Z. H. Mahmood and M. K. Ibrahem, (2018) "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing," IEEE (AiCIS), pp. 182-186.

[15]. G. Raj, R. C. Kesireddi and S. Gupta, (2015) "Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud," IEEE (NGCT), pp. 374-378.

[16]. K. Rani and R. K. Sagar, (2017) "Enhanced data storage security in cloud environment using encryption, compression and splitting technique," IEEE (TEL-NET), pp. 1-5.

[17]. Y. S. Gunjal, M. S. Gunjal and A. R. Tambe, (2018) "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing", IEEE (ICACCT), pp. 187-190.

[18]. V. Sreenivas, (2013) "Performance evaluation of encryption techniques and uploading of encrypted data in cloud", IEEE (ICCCNT), pp. 1-6.

[19]. P. More, S. (2018) "Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud", IEEE (ICACCT), pp. 93-96.

[20]. W. Chen, (2018) "Efficient Key-Aggregate Proxy Re-Encryption for Secure Data Sharing in Clouds", IEEE (DSC), pp. 1-4.

[21]. N Pradheep, M Venkatachalam, M Saroja, S Prakasam, (2017) "A Cloud Computing Solution for Securely Storing and Accessing Patients Medical Data", Journal of Advanced Research in Dynamical and Control Systems, pp. 614-622.

[22]. P. L. R. Chze and K. S. Leong, (2014) "A secure multi-hop routing for IoT communication," IEEE (WF-IoT), pp. 428-432.

[23]. G. Hatzivasilis, I. Papaefstathiou and C. Manifavas, (2017) "SCOTRES: Secure Routing for IoT and CPS," IEEE Internet of Things Journal, Vol. 4, Iss. 6, pp. 2129-2141.

[24]. A. E. Hajjar, G. Roussos and M. Paterson, (2017) "Secure routing in IoT networks with SISLOF," Global Internet of Things Summit (GIoTS), pp. 1-6.

[25]. Shengli Mao, (2018) "Crowd cloud routing protocol based on opportunistic computing for wireless sensor networks", EURASIP Journal on Embedded Systems, Volume 2016, Number 01, pp. 1-7.

[26]. Uma Khemch and Thakur, (2019) "QoS Aware Cloud Based Routing Protocol for Security Improvement of Hybrid Wireless Network", Machine Learning Research, Volume 4, Issue 1, pp 21-26.

[27]. Mahalakshmi Jeyabalu, (2013) "A Survey on Routing Algorithms for Cloud Computing", IJCA, Number 4, 2013, pp. 1-7.

[28]. Mohsin Nazir, (2012) "Cloud Computing: Overview & Current Research Challenges," IOSR-JCE, Volume 8, Issue 1, PP 14-22.

[29]. Deepa Mehta, (2017) "Routing Optimization in Cloud Networks", IJARCS, Volume 8, Number 2, pp. 16-18.

[30]. Kazi Masum Sadique, (2018) "Towards Security on Internet of Things: Applications and Challenges in Technology", Procedia Computer Science, Volume 141, 2018, PP 199-206.

[31]. D. Airehrour, J. Gutierrez and S. K. Ray, (2016) "A Lightweight Trust Design for IoT Routing, (DASC/PiCom/DataCom/CyberSciTech), pp. 552-557.

[32]. A. E. Basabi, Jingsha He and S. M. Hashemi, (2016) "Secure routing in IoT with multi-objective simulated annealing," IEEE (ICCC), pp. 2073-2076.

[33]. G. Glissa, A. Rachedi and A. Meddeb, (2016) "A Secure Routing Protocol Based on RPL for Internet of Things," IEEE (GLOBECOM), pp. 1-7.

[34]. Chaithra .S, (2016) "Study of Secure Fault Tolerant Routing Protocol for IoT", IJSR, Volume 5, issue 7, 2016, pp. 1833-1838.

[35]. Gholamreza Ramezan, A Blockchain, (2018) "Based Contractual Routing Protocol for the Internet of Things Using Smart Contracts", Wireless Communications and Mobile Computing, pp. 1-14.