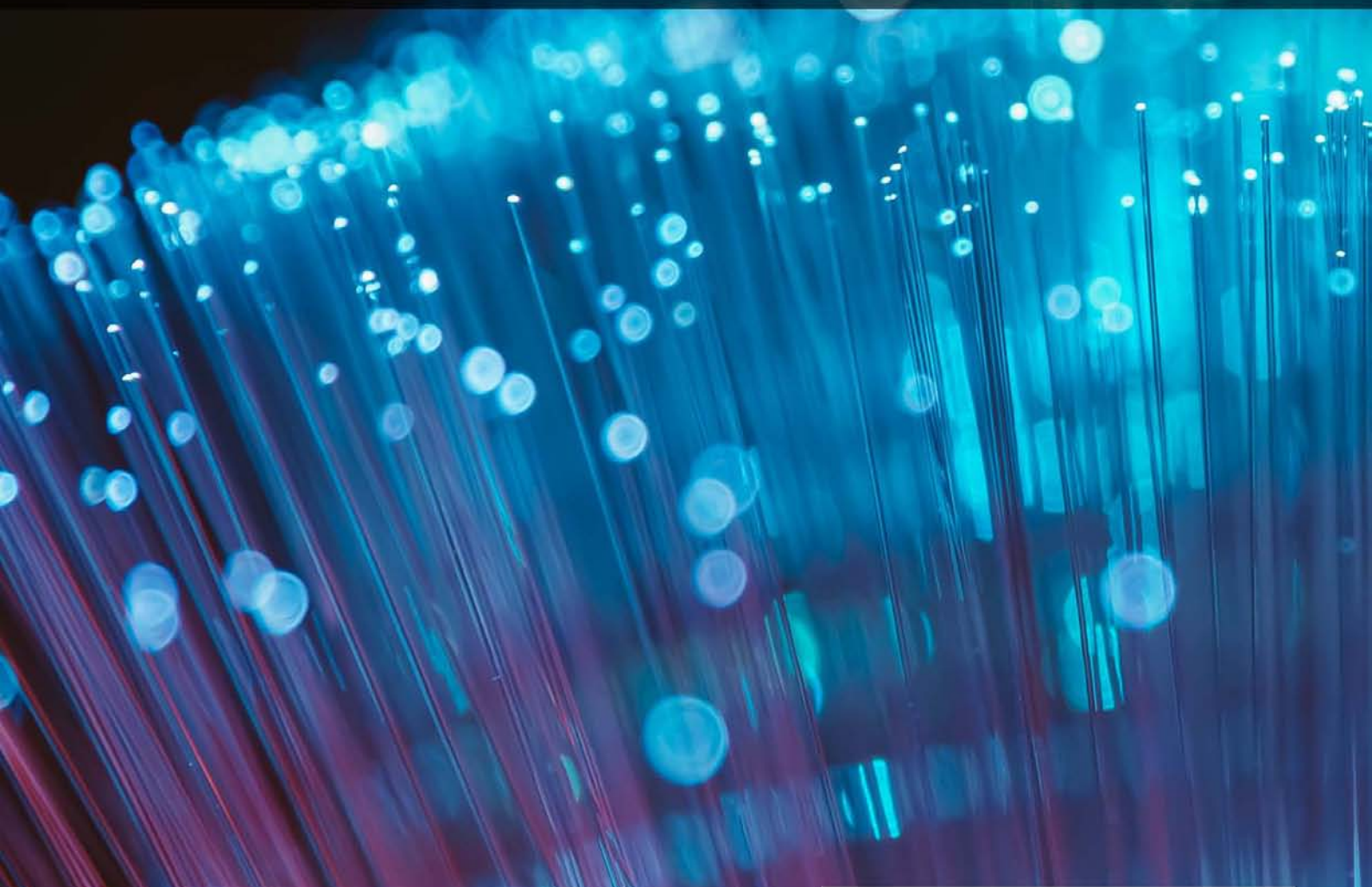
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security



Anomaly Intrusion Detection

Wireless Sensor Network for IoT

Highlights

ERP Security Based on Web

Agriculture Growth using Wireless

Discovering Thoughts, Inventing Future

VOLUME 20 ISSUE 2 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 20 Issue 2 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Dr. Stefano Berretti

Ph.D. in Computer Engineering and Telecommunications, University of Firenze Professor Department of Information Engineering, University of Firenze, Italy

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department Youngstown State University Ph.D., Texas A&M University University of Missouri, Columbia Gazi University, Turkey

Dr. Lamri Sayad

Ph.d in Computer science, University of BEJAIA, Algeria

Dr. Tauqeer Ahmad Usmani

Ph.D in Computer Science, Oman

Dr. Hazra Imran

Ph.D in Computer Science (Information Retrieval), Athabasca University, Canada

Dr. Magdy Shayboub Ali

Ph.D in Computer Sciences, MSc in Computer Sciences and Engineering, BSc in Electronic Engineering, Suez Canal University, Egypt

Dr. Nurul Akmar Binti Emran

Ph.D in Computer Science, MSc in Computer Science, Universiti Teknikal Malaysia Melaka, Malaysia

Dr. Asim Sinan Yuksel

Ph.D in Computer Engineering, M.Sc., B.Eng., Suleyman Demirel University, Turkey

Dr. Anis Bey

Dept. of Computer Science, Badji Mokhtar-Annaba University, Annaba, Algeria

Alessandra Lumini

Associate Researcher Department of Computer Science and Engineering University of Bologna Italy

Dr. Rajesh Kumar Rolen

Ph.D in Computer Science, MCA & BCA - IGNOU, MCTS & MCP - MIcrosoft, SCJP - Sun Microsystems, Singhania University, India

Dr. Rajneesh Kumar Gujral

Ph.D in Computer Science and Engineering, M.TECH in Information Technology, B. E. in Computer Science and Engineering, CCNA Certified Network Instructor, Diploma Course in Computer Servicing and Maintenance (DCS), Maharishi Markandeshwar University Mullana, India

Dr. Aziz M. Barbar

Ph.D. IEEE Senior Member Chairperson, Department of Computer Science AUST - American University of Science & Technology Alfred Naccash Avenue Ashrafieh, Lebanon

Dr. Federico Tramarin

Ph.D., Computer Engineering and Networks Group, Institute of Electronics, Italy Department of Information Engineering of the University of Padova, Italy

Dr. Chutisant Kerdvibulvech

Dept. of Inf. & Commun. Technol., Rangsit University Pathum Thani, Thailand Chulalongkorn University Ph.D. Thailand Keio University, Tokyo, Japan

Dr. Roheet Bhatnagar

Ph.D in Computer Science, B.Tech in Computer Science, M.Tech in Remote Sensing, Sikkim Manipal University, India

Contents of the Issue

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 2 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Optimized Load Centroid and Rabin Onion Secured Routing in Wireless Sensor Network for IoT

By Renuka Mohanraj
Maharishi International University

Abstract- Advances in wireless communication have geared up extensive insights wherein the sensors can themselves communicate with other sensors that form significant parts of the Internet of Things (IoT). However, the large-scale acceptance of WSN for IoT is still surfacing threats and controversies that apprehend the security aspects. There are a lot of attacks that can manipulate the routein WSN for IoT. In this work, an Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method are designed to improve the throughput rate with minimum routing overhead and latency. The proposed method is based on a Centroid and Rabin Signature, a Digital Signature technique. First, the optimal route is identified by considering both the load and residual energy using Load Centroid function. Then onion routing is used for selecting secured route amongst the optimality. Besides, the node genuineness is checked by applying the Rabin Signature.

Keywords: wireless sensor network, internet of things, security, load centroid, rabin signature, onion routing.

GJCST-E Classification: C.2.1

Strictly as per the compliance and regulations of:

Optimized Load Centroid and Rabin Onion Secured Routing in Wireless Sensor Network for IoT

Renuka Mohanraj

Abstract- Advances in wireless communication have geared up extensive insights wherein the sensors can themselves communicate with other sensors that form significant parts of the Internet of Things (IoT). However, the large-scale acceptance of WSN for IoT is still surfacing threats and controversies that apprehend the security aspects. There are a lot of attacks that can manipulate the routein WSN for IoT. In this work, an Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method are designed to improve the throughput rate with minimum routing overhead and latency. The proposed method is based on a Centroid and Rabin Signature, a Digital Signature technique. First, the optimal route is identified by considering both the load and residual energy using Load Centroid function. Then onion routing is used for selecting secured route amongst the optimality. Besides, the node genuineness is checked by applying the Rabin Signature. Each node uses a special data structure (i.e. onion routers) to store routing information. The main objective of this algorithm is to improve security and efficiency for WSN in IoT. The performance of the proposed Optimized Load Centroid and Rabin Onion Secured Routing method is compared with different state-of-the-art methods using the NS-2 simulator. Extensive simulation scenarios are considered, and final results show that the proposed method has higher throughput with minimum routing overhead and route acquisition latency, which makes it more efficient in WSN for IoT.

Keywords: wireless sensor network, internet of things, security, load centroid, rabin signature, onion routing.

I. Introduction

The Internet of Things (IoT), where several devices are associated to share the data in different domains such as home automation, patient monitoring, industrial device monitoring, smart cities, and so on. Wireless Sensor Networks (WSNs), due to its ubiquitous devices, has been in use in recent years in many IoT applications. However, researchers have not complicatedly addressed the issue part during routing. A significant amount of research work in the domains of security, topology, and energy consumption in WSN for IoT has been managed in the recent past.

Given view of the essential qualities of the sensor nodes in WSN, the constrained computing capability, and energy requirements, a Sector-based Random Routing (SRR) method was presented in [1] to address the Source Location Privacy (SLP) issues and therefore minimizing the energy consumption. With this objective, in SRR, the data packets were sent to random phantom sources that were situated in several sensors. These were then disseminated via all routes to arrive promptly at the sink node. Besides, the notion of a hop threshold was also included to manage the routing strategies and minimize energy consumption.

Despite improvement observed in the energy consumption with minimum delay, the routing overhead was not considered. To minimize the routing overhead, the Load Centroid Optimal Route Identification model is applied to the WSN network that considers both load and residual energy to identify optimal routes.

An Anchor-based Routing method was designed in [2] with constrained flooding and dynamic clustering. A novel type of event-based clustering model along with a novel clustering mechanism to be included dynamically. With the design of these models, energy consumption was said to be reduced with higher number of packets processed successfully by the sink. Data collection performed at the mobile sink was then said to be shared to the contended users via IoT infrastructure.

Despite the improvement observed in the throughput rate, the security aspect was not covered. To improve the security with minimum latency and higher throughput, in this work, a Rabin Onion Secured Routing algorithm is designed. This algorithm not only identifies the secured route using Onion Routing but also ensures that the node with which the routing is carried out is also authenticated node or in other words, the genuineness of the node is checked via Rabin Signature.

In this paper, we propose an optimal and secured routing to be followed in WSN for IoT, called Optimized Load Centroid and Rabin Onion Routing (OLC-ROR). OLC-ROR method aims at ensuring the routing overhead for IoT-based applications, i.e., for a smart city. To improve the efficiency of the throughput rate, the OLC-ROR method analyzes onion routes for obtaining secured routing and builds an Onion-based Route in WSN for IoT. Also, in contrast to existing anchor-based routing, OLC-ROR method leverages a Rabin Onion Secured Routing algorithm to ensure route

Author: Department of Computer Science, Maharishi International University, Fairfield, Iowa, USA. e-mail: rmohanraj@miu.edu

acquisition latency. Our selection secured routing algorithm is performed based on the Rabin signatures with minimum load and residual energy and, can reduce the routing overhead of the entire smart city network.

The main contributions of the proposed work are summarized as follows:

- We design a Load Centroid function that is exploited as the basis of constructing an optimal routing model to reduce the routing overhead.
- We identify serious security threats to the optimal routing in WSNs for IoT. Subsequently, a Rabin Onion Secured Routing algorithm is introduced to obtain secure routes with minimum route acquisition latency.
- A Rabin Signature is exclusively proposed to verify the genuineness of the node with which secured routing is said to be established, at the same time it also significantly improves the throughput rate incur by the secured routing.
- Theoretical analysis and empirical validations are done to show the significance of OLC-ROR method. It reduces the routing overhead and route acquisition latency with higher throughput rate.

The paper is prearranged in the following sections. Section 2 describes the work related to security aspects in WSN for IoT. Section 3portrays the method of secure routing, Optimized Load Centroid and Rabin Onion Routing (OLC-ROR). The simulation setup, along with the results, is depicted in Section 4 and Section 5, respectively. Finally, the concluding remarks are shown in Section 6.

II. Related Works

Adding the distinctiveness and the extent of the routing path can significantly improve the network safety time. But, the constrained energy consumption has to be also considered. In [3], a source location privacy protection scheme based on ring-loop routing (SLPRR) in WSNs for IoT was presented to solve the issues related to energy consumption. Three types of routing were first considered, followed by which the distinctiveness and routing extent were said to be enhanced. Finally, rings were formed in the non-hotspot area, therefore reducing energy consumption.

With new improvements in IoT technology, authorized users are said to access reliable sensor nodes. By accessing the reliable sensor nodes, data are said to be first obtained, and commands are also sent to the destined nodes. However, designing an effectively secured authentication and key agreement scheme is significant due to the resource constrained nodes. In [4], secure and lightweight authentication and key agreement scheme for IoT based WSNs were designed, contributing to the security aspect.

A survey on recent advancements in data trust, communication trust in WSN-assisted IoT was designed [5]. However, security for both data and route was not ensured. To address this issue, a cross-layer based adaptive secured routing and data transmission process was designed in [6] to ensure data security.

With the routing protocol susceptible to different types of attacks in WSN, which is an important network type of IoT. The correlation coefficient, and Kolmogorov-Smirnov (KS) test approaches were combined to measure the trustworthiness of the Intrinsic Mode Function (IMF) components and discard the false IMF components. Besides, Hilbert-Huang transformation and trust evaluation techniques [7] were also integrated to cover the security aspect.

However, with the IoT edge nodes being exposed to different types of attacks, in [8], the focus was made on developing a lightweight authentication model for constrained end-devices, therefore ensuring security. Yet another convolutional technique concentrating on security aspect was designed in [9] to prevent malicious node attacks.

A full evaluation of security attacks regarding WSNs and IoT, along with the methods to detect the types of attack, preventing the attacks, and mitigations of those attacks was presented in [10]. IoT is not only considered as the most favorable research topic but also considered as the blossoming industrial drift. The basic idea in the Internet is to bring objects; there are different methods because an IoT system is introduced in several applications. A WSN based IoT platform for wide-area and heterogeneous sensing applications was presented in [11].

A concept of combining fault tolerance and secured routing model in WSN called as the Fault Tolerant Secured Routing (FASR) that ensures secured routes between the source node and sink nodes under faulty node constraints was presented in [12]. Here, faulty nodes were first identified via battery power and interference models. Next, the trustworthy nodes between fault-free nodes were then obtained using agent-based trust model. Finally, the data was found to be secured routed via fault-free non-compromised nodes to sink. Yet another secured and effective access control mechanism for WSN in the cross-domain context of the IoT [13] that permits an Internet user in Certificate Less Cryptography (CLC) environment to communicate with a sensor node via an Identity-Based Cryptography (IBC) environment with different system parameters.

A secure routing and monitoring model via multiple variant tuples using the Two-Fish (TF) symmetric key approach to identify and discard the malicious nodes in the network was designed in [14] based on the Authentication and Encryption Model (ATE). With the aid of the Eligibility Weight Function (EWF), the sensor guard nodes were identified and were hidden using a symmetric key approach. However, challenges posing security for the smart city was less focused. In [15], a scalable framework for authentication

and hierarchical routing was designed to address the security issues. However, the energy efficiency of the node was not concentrated. In [16], presented an energy-aware and secure multi-hop routing protocol using a secret sharing scheme. So that reduces the energy consumption along with the network throughput and average end-to-end delay.

An enhancement of the reactive routing protocol, called constrained flooding and dynamic clustering, was presented in [17]. Here, a novel event-based clustering mechanism, in addition to the dynamic clustering technique, minimizing the energy consumption with higher data packets being processed successfully manner to the sink node.

In [18], the networking characteristics required for smart city applications, besides networking protocols utilized to engage different data traffic streams, were introduced. A secure 3-way routing protocol for routing using cryptographic techniques for providing a high degree of security was introduced in [19].

For the influence of constrained energy and networking attacks resulted from open transmission channels, a low-power and secure multi-hop routing technique based on the Markov state transition theory was presented in [20]. Here, with the random transmission route selection, typical attacks were said to be eliminated, thus resulting in secured data transmission with the reduced energy consumption.

All the existing methods are given above utilized random route selection and balanced load to secure data transfer. Random route selection is not an effective approach as it consumed more routing overhead and route acquisition latency to generate the route according to load factor. Each node entering the network is provided with these load factors; therefore, for large networks it becomes more complex and more storage space is required, which is limited. In the proposed method, an optimal routing model is used to select the optimal route using minimum load centroid and residual energy and hence minimizing the routing overhead. Next, a secure route is obtained via onion routers, and node authentication is also checked using Rabin signature.

III. Methodology

In this section, an optimal and secured routing method to be followed in WSN for IoT called Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) is designed. Here, two different models are used. First, optimal route identification is made by applying the Load Centroid function. The objective behind the use of the Load Centroid function is that it assists in minimizing the routing overhead because of the consideration of both minimum load and residual energy while selecting the route. Next, amongst optimal routes being identified, secured routing is followed by applying the Rabin Onion Routing model. The purpose of using this routing model is that by using Onion routing, the route acquisition latency is reduced, and using Rabin Signature, verification is performed, therefore ensuring security with a higher throughput rate. First, a network model used for the design of OLC-ROR is presented, followed by which the elaborate description is provided.

a) Network model

Let us assume a multi-hop WSN that comprises a number of sensor nodes $N = N_1, N_2, \ldots, N_n$, and some sink nodes $S = S_1, S_2, \ldots\ldots, S_n$ is deployed for one application (i.e., for a smart city) of IoT. The sensor nodes deployed in WSN within the wireless transmission range ' R ' directly send data packets $DP = DP_1, DP_2, .., DP_n$ to each other following a specified type of routing. The multi-hop communication is said to be enabled when the distance is said to be greater than the transmission range with the assumption that the sensor node in the network is a dense network where each sensor node has several neighbor nodes.

Thus, this network is said to be defined by a graph $G(V, L)$. Here, V represents the set of sensor nodes and, L represents the set of links between the sensor nodes in the network. Besides, a link is represented by $link_{i,j} \in L$, if the distance between the sender nodes $i \in V$ and the receiver node $j \in V$ is smaller than the transmission range R. Figure 1, given below illustrates a sample IoT-based WSN.

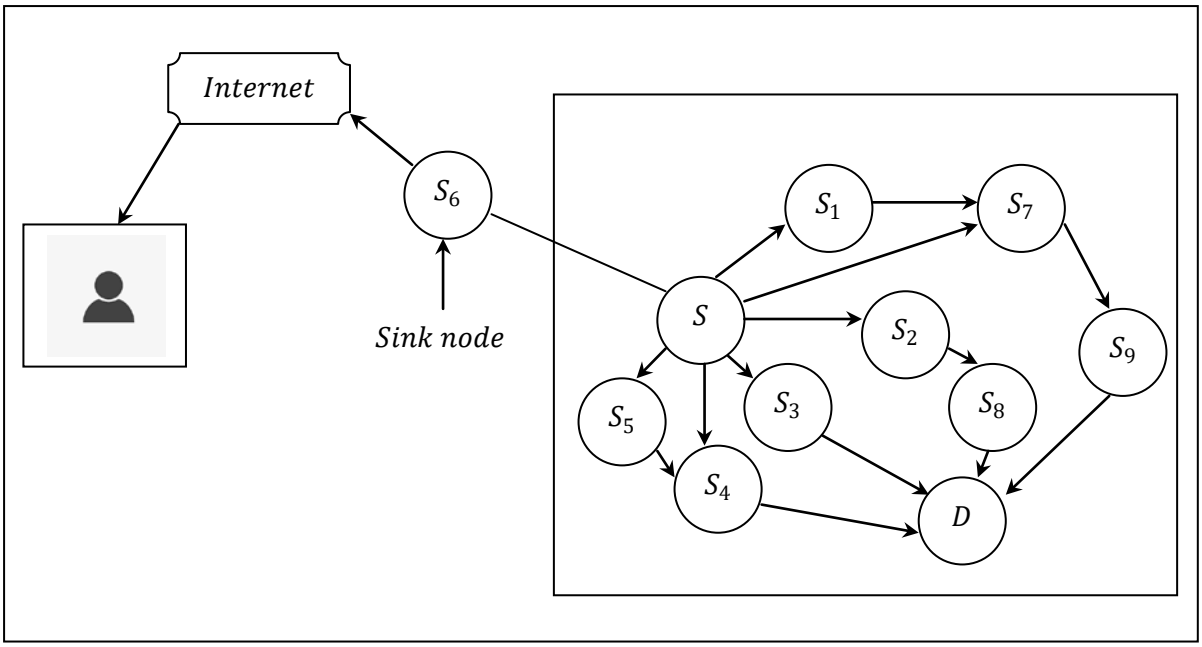


Figure 1: IoT-based WSN

Figure 1 given above depicts a scenario of WSN in IoT with a single source node S, single destination node D, with multiple sensor nodes 'S_1', 'S_2', 'S_3', 'S_4', 'S_5', 'S_7', 'S_8', 'S_9', one sink node 'S_6'respectively that also acts as the gateway node. Therefore, multiple sensor nodes join the internet through a gateway or sink node. In this work, an IoT-enabled WSN for a smart city is designed that uses different types of IoT sensors for route optimization and secured routing.

b) Load Centroid Optimal Route Identification

In an IoT-enabled WSN, different routes are said to exist with the advantages of following one route over another route. Therefore, multiple routes are said to exist for an IoT-enabled WSN. However, the optimal route has to be identified. In this section, Optimal Route Identification is said to be made using Load Centroid function. Table 1, given below shows the sample routes identified for figure 1.

Table 1: Sample Routes

Number of Routes identified	Routing Pattern
R_1	$S \rightarrow S_2 \rightarrow S_5 \rightarrow D$
R_2	$S \rightarrow S_4 \rightarrow D$
R_3	$S \rightarrow S_3 \rightarrow D$
R_4	$S \rightarrow S_7 \rightarrow S_9 \rightarrow D$
R_5	$S \rightarrow S_1 \rightarrow S_7 \rightarrow S_9 \rightarrow D$
R_6	$S \rightarrow S_5 \rightarrow S_4 \rightarrow D$

In the field of mathematics, centroid refers to the center of the load, the imaginary point of mass concentration.With the sample routes identified, in our study, the concept of Load Centroid is used to identify the optimal route. So, the route with minimal load and average residual energy is said to be an optimal route when compared to the other routes. Figure 2 shows the block diagram of the Load Centroid Optimal Route Identification model.

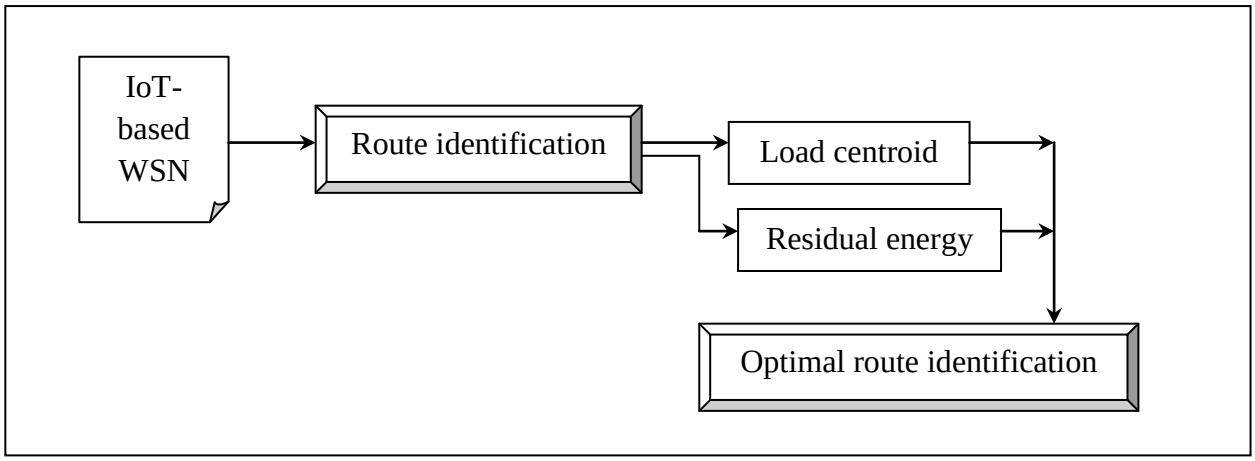


Figure 2: Block diagram of Load Centroid Optimal Route Identification

As depicted in the above figure 2, the first optimal route identification is performed by applying Load Centroid function along with the residual energy. The pseudo-code representation of load-balanced optimal route identification using Load and residual energy centroid function is given below.

Input: Sensor nodes '$S = S_1, S_2, \ldots, S_n$', Source node '$S$', Destination node '$D$'
Output: Load balanced optimal route identification '$R = R_1, R_2, \ldots, R_n$'
1: **Begin** 2: **For** each sensor nodes '$S = S_1, S_2, \ldots, S_n$' with source node '$S$', destination node '$D$' 3: Measure position of the load centroid with respect to 'P' axis using (1) 4: Measure position of the load centroid with respect to 'Q' axis using (2) 5: Measure residual energy centroid with respect to 'P' axis using (3) 6: Measure residual energy centroid with respect to 'Q' axis using (4) 7: Return (load balanced optimal route) 8: **End for** 9: **End**

Algorithm 1: Load Centroid Optimal Route Identification

As given in the above algorithm, for each sensor nodes with source node requesting to send the data packets, the position of load centroid, followed by residual energy centroid are measured. The equations (1) and (2) given below are utilized to measure the position of the load centroid and is formulated as given below.

$$P_{lc} = \frac{SM_q}{SM} = \frac{\int p * \alpha DL}{\int \alpha DL} \quad (1)$$

$$Q_{lc} = \frac{SM_p}{SM} = \frac{\int q * \alpha DL}{\int \alpha DL} \quad (2)$$

From the above equations (1) and (2), $P, Q,$ represents the coordinates of the node i, P_{lc} and Q_{lc} symbolizes the results of load coordinates with α representing the node density, SM_q, SM_p representing the static moment to the q axis and p axis for a differential of load DL respectively. Then, the residual energy centroid rec for two different axes P and Q is measured as given below.

$$P_{rec} = \frac{\sum_{i=0}^{n} \frac{E_{i\_re}}{E_{ie}} * P}{N} \quad (3)$$

$$Q_{rec} = \frac{\sum_{i=0}^{n} \frac{E_{i\_re}}{E_{ie}} * Q}{N} \quad (4)$$

From the above equations (3) and (4), E_{i_re}, represents the residual energy of node i with an initial energy of E_{ie} respectively. If the load of the sensor nodes is known and said to be distributed in an even fashion, then equations (3) and (4) are used to measure the position of the load centroid. However, for IoT-based WSN, the influence of node load in the network is not required for the network lifetime. Therefore, with the node load information and the residual energy, the equations (3) and (4) are used to measure the position of the residual energy centroid.

Therefore, the residual energy centroid has the influence of the energy distribution during the smooth operation of the network. Hence, in this work, both the load and residual energy centroid are considered in an integrated manner to select the optimal route. With this, the routing overhead incurred in identifying the optimal route is said to be reduced. Table2, given below shows the optimal routes identified after applying the load centroid function.

Table 2: Load Centroid Optimal Routes

Number of Routes identified	Routing Pattern
R_2	$S \rightarrow S_4 \rightarrow D$
R_3	$S \rightarrow S_3 \rightarrow D$

c) Rabin Onion Secured Routing

Smart security is an essential component of IoT-based WSN. Since IoT-based WSN uses the wireless medium, communication in a wireless network can arise from any direction and can target any node, therefore it ranges from different types of attacks, and securing smart cities for the future remains a key concern. There are a few solutions for securing routing protocols for IoT-based WSN as far as a smart city is concerned. But still due to security lapse while routing and detecting them is complicated in IoT-based WSN.

The goal here is to propose a model that performs point-to-point routing authentication with IoT-based WSN. There is another issue of plotting secure and efficient routing protocols that have both high network performance via route acquisition latency and security with a higher throughput rate. Although the researcher has outlined several security mechanisms for a few existing secured routing protocols. Yet, there is no standard secured routing model for IoT-based WSN that performs best regarding performance (i.e., minimum route acquisition latency) and performance (i.e. maximum throughput rate).

In this work, with the objective of securing both the route and the carrier node, a Rabin Onion Secured Routing algorithm is designed. The proposed routing algorithm is to select a secured route while considering the key when selecting the forwarding route. Also, carrier node genuineness is a key requirement for IoT-based WSN. Thus, we also propose a model to balance between throughput and route acquisition latency in our Rabin Onion Secured Routing model.

Rabin Onion Secured Routing ensures anonymous communication over a computer network, where the nodes are encapsulated in layers of encryption, related to the layers of an onion. The encrypted data is transmitted through a series of intermediate or relay nodes called onion routers, uncovering the data's next destination. When the final node is decrypted, the data packet arrives at its destination, ensuring both secured routing with the correctness of carrier node genuineness. The sender node is said to be anonymous because each intermediate node knows only the location of the immediately preceding and following nodes. Figure 3 shows the block diagram of Rabin Onion Secured Routing.

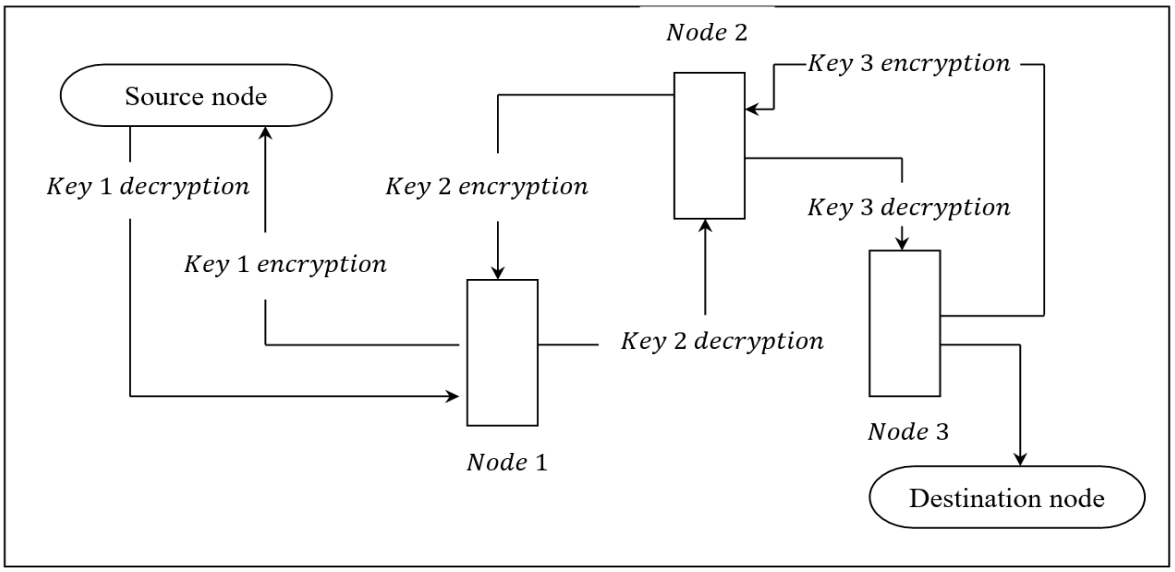


Figure 3: Rabin Onion Secured Routing

Figure 3 shows a Rabin Onion Secured Routing model followed for IoT-based WSN with a sample of three intermittent nodes between the source and destination node. This onion secured routing model is applied once the optimal routes are said to be identified. With the optimal routes, secured routing amongst them is identified by following onion routing. The source node with access to all the encryption keys, i.e., $K = K_1, K_2, \ldots, K_n$ encrypts the message wrapping it under three layers like an onion.

This triple encrypted layer message is then sent to the first intermediate node N_1. Here, N_1 only has the address of N_2 and K_1. Hence, it decrypts the message using K_1 and perceives that it does not make any sense since it still has two layers of encryption. So, it passes it on to N_2. Here, N_2 has K_2 and the addresses of the input & exit nodes. So, it decrypts the message using K_2 perceiving that it is still encrypted and passes it onto the exit node. Now, the N_3 peels of the last layer of encryption and pass it on to the destination node.

The destination node processes the request and serves up the desired source node as a response. The response passes through the same sensors in the opposite direction where each node puts on a layer of encryption using their specific key. It finally reaches the source node in the form of a triple encrypted response that is said to be decrypted as the source node has access to all the keys. The pseudo-code representation of Rabin Onion Secured Routing is given below.

Input: Optimal routes '$R = R_1, R_2, \ldots, R_n$', sensor nodes '$S = S_1, S_2, \ldots, S_n$', source node '$S$', destination node '$D$', encryption keys, '$K = K_1, K_2, \ldots, K_n$'

Output: Robust secured routing '$SR = SR_1, SR_2, \ldots, SR_n$'

1: **Begin**
2: For each Optimal routes 'R', with sensor nodes 'S' with encryption keys, 'K'
3: For each source node 'S' with destination node 'D'
4: Select public key and private key using (6) and (7)
5: Solve the rabin function using (9)
6: Measure the genuineness of intermediate node via
7: If '$x(x+u), mod\ f = (DP * RP\ mod\ f)$'
8: Node said to be genuine
9: Perform secured routing
10: **End if**
11: **If** '$x(x+u), mod\ f <> (DP * RP\ mod\ f)$'
12: Node said to be not genuine
13: Go to step 4
14: **End if**
15: **Return** (Robust secured routing 'SR')
16: **End for**
17: **End for**
18: **End**

Algorithm 2: Rabin Onion Secured Routing

As given in the above algorithm, for each Optimal route$R$, with source node S destination node D, the source node S selects primes a, b and measures the product as given below.

$$f = a * b \tag{5}$$

With the measured product, the source node S, then chooses a random u in $\{1,2, \ldots, f\}$ with public key PB_{Key} and private key PR_{Key} as given below.

$$PB_{Key} \rightarrow (f, u) \tag{6}$$

$$PR_{Key} \rightarrow (a, b) \tag{7}$$

To send a data packet DP, the source node S picks random padding $RP$and is written as given below.

$$fun = DP * RP\ mod\ f \tag{8}$$

Then, the source node solves the Rabin Signature written as given below.

$$RS = x(x+u), mod\ f = (DP * RP\ mod\ f) \tag{9}$$

The signature on DP is the pair (RP, x). Finally, authentication of the sensor is performed via verifying the genuineness of the node. Given a data packet DP, and a signature (RP, x), the verifier calculates $x(x+u), mod\ f$ and $(DP * RP\ mod\ f)$ and verifies that they are equal. Hence, by applying Rabin Onion Secured Routing, both the secured routes obtained via Onion Routing, and the genuineness of the selected routing node is verified using Rabin Signature. Therefore, both the route acquisition latency is said to be reduced and throughput rate is improved, ensuring secured routing.

IV. Simulation Setup

The performance of the Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method is evaluated in this section. Simulations were carried out to compare the performance of the OLC-ROR method. The following results compare the performance characteristics of Sector-based Random Routing (SRR) [1] method, Anchor-based Routing [2] method with proposed OLC-ROR method in a simulated environment. In our implementation, sensor nodes are placed randomly in the network of 1000m * 1000m. Each simulation result is based on ten iterations. The practical networks include a notable number of malicious nodes, and their consequences have to be circumvented. The results are summarized in Table. The version of NS-2 used in our simulation is NS-2.35.

Table 3: NS-2 Simulation parameters

Parameters	Description
Network size	1000m * 1000m
Total number of nodes	50, 100, 150, 200, 250, 300, 350, 400, 450, 500
Simulation time	100s
Max node speed	20 km/hr
Initial energy	2J
Traffic source	Constant Bit Rate
Packet size	512 bytes
Radio range	250m
Mobility	Random way point
Node's transmission range	25m

In the network scenario, 500 sensor nodes were deployed of homogeneous characteristics. Initially, all nodes have 2J energy levels, whereas the transmission power for each node is fixed to 25m. The proposed method is compared with [1] and [2], and the performance is evaluated in terms of routing overhead, route acquisition latency, and throughput.

V. Discussion

This section presents the performance evaluation of the Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method. Its effectiveness is analyzed for secured routing in WSN for IoT that represents a dense IoT routing with sensor networks. Here, we show how with the aid of OLC-ROR method can follow optimal routing where there are several sensors. Furthermore, we compared the OLC-ROR method with that of SRR [1] and Anchor-based Routing [2] for ensuring secured routing for IoT once all the three methods have a common goal to detect optimal route and also we can show improvement from OLC-ROR compared to the previous work.

a) *Performance analysis of routing overhead*

The first metric considered for analysis is the routing overhead. Whenever an optimal route has to be found, a considerable amount of overhead is said to be incurred. Lower the routing overhead, more efficient and optimal the route is said to be and vice versa. The routing overhead is written as given below.

$$RO = \frac{DP_{tot} + CM_{tot}}{DP_{tot}} \quad (10)$$

From the above equation (10), the routing overhead RO refers to the ratio of summation of the total passed data packets DP_{tot} and the total control messages CM_{tot} to the total passed data packets DP_{tot} respectively. Let us consider 1000 data packets with different types of IoT sensors in a smart city environment, and let us assume the 100 control packet. Then, the routing overhead using the proposed OLC-ROR, SRR [1], and Anchor-based Routing [2] is measured as given below.

Sample calculation for routing overhead

- Proposed OLC-ROR: With 25 number of totals passed data packets and 20 number of total control messages, the routing overhead measured is given below.

$$RO = \frac{25 + 20}{25} = 1.8$$

- Existing SRR: With 25 number of totals passed data packets and 21 number of total control messages, the routing overhead measured is given below.

$$RO = \frac{25 + 21}{25} = 1.84$$

- Existing Anchor-based Routing: With 25 number of totals passed data packets and 22 number of total control messages, the routing overhead measured is given below.

$$RO = \frac{25 + 22}{25} = 1.88$$

Table 4, given below shows the tabulation results of routing overhead for variant number of packets considered in the range of 25 to 250 for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2].

Table 4: Tabulation for routing overhead

Number of packets	Routing overhead (ratio)		
	OLC-ROR	SRR	Anchor-based Routing
25	1.8	1.84	1.88
50	2.1	2.3	3.1
75	2.4	2.7	3.3
100	2.5	3	3.8
125	2.8	3.3	4.1
150	3.1	3.8	4.5
175	3.3	4.1	5
200	3.5	4.5	5.3
225	4.1	5	5.5
250	4.5	5.3	5.9

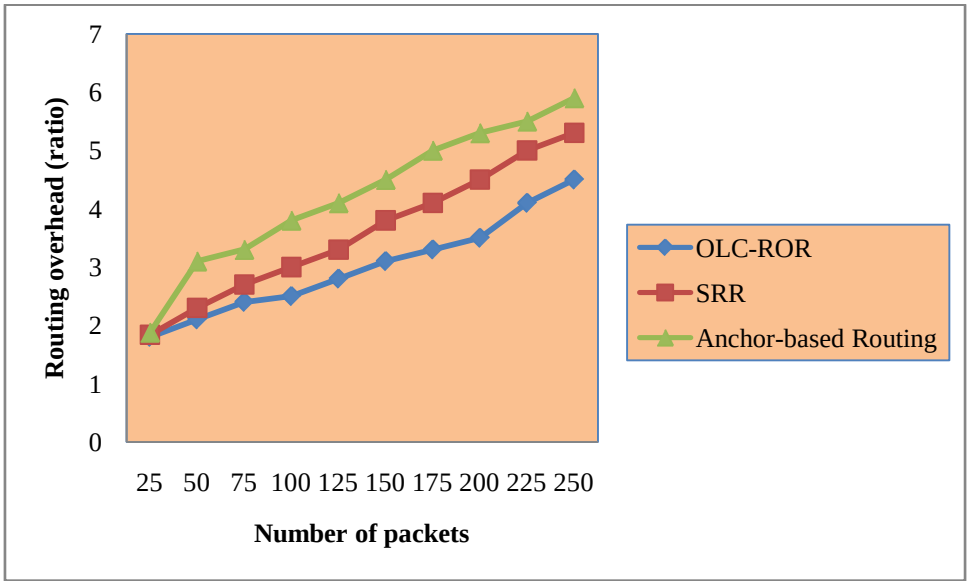


Figure 4: Measure of routing overhead over number of packets

The Figure given above shows the routing overhead for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2]. The number of packets is varied in the range of 25 to 250 for ten different simulation runs with each packet varying in the size of 512 bytes. Routing overhead refers to the number of routing packets required for network communication. The proposed algorithms used for routing produces a considerable number of small-sized packets and are referred to as the routing packets. However, routing packets do not carry any application content, as in the case of the data packets. But routing packets and the data packets shares the same network bandwidth, and therefore routing packets are considered as an overhead in the WSN. This overhead is referred to as the routing overhead, lesser the routing overhead, efficient is the method said to be. Figure 4 shows the RO of the three methods. The RO is found to be reduced when applied with the OLC-ROR method when compared to [1] and [2]. The improvement or the minimization of routing overhead using the OLC-ROR method is due to the application of the Load Centroid Optimal Route Identification algorithm. By applying this algorithm, both position of the load centroid and residual energy centroid is considered while selecting the optimal route. Therefore, a route possessing minimal load and lesser residual energy is selected as an optimal route via load and residual energy centroid function. Proposed method minimizes the routing overhead by 15% when compared to [1] and 28% when compared to [2].

b) The Performance measure of routing acquisition latency

The second metric used while considering secured routing in WSN for IoT is the route acquisition

latency. It is measured in terms of milliseconds (ms). It refers to the average time consumed between the generation of a Rabin signature and the reception of the first valid route produced from an intermediary device. Route acquisition latency is calculated only for the Rabin signatures of data packets successfully received by the sink node. It is measured as given below.

$$RAL = \sum_{i \in N}(T_{i,res}) - (T_{i,req}) * N \quad (11)$$

From the above equation (11), the route acquisition latency RAL is measured based on the time at which a signature is generated to request a route for data packet $T_{i,req}$ and $T_{i,req}$ refers to the time at which the first valid route offer for data packet i is received by the source IoT device and N is the number of nodes in the network. The sample calculations for route acquisition latency using the proposed OLC-ROR, existing SRR [1], and existing Anchor-based Routing [2] is given below.

Sample calculations for route acquisition latency

- Proposed OLC-ROR: With 50 number of nodes considered for simulation and $0.035ms$ refers to the time between the request and response, the route acquisition latency is measured as given below.

$$RAL = 0.035ms * 50 = 1.75ms$$

- Existing SRR [1]: With 50 number of nodes considered for simulation and $0.055ms$ refers to the time between the request and response, the route acquisition latency is measured as given below.

$$RAL = 0.055ms * 50 = 2.75ms$$

- Existing Anchor-based Routing [2]: With 50 number of nodes considered for simulation and $0.075ms$ refers to the time between the request and response, the route acquisition latency is measured as given below.

$$RAL = 0.075ms * 50 = 3.75ms$$

Table 5 given below, shows the tabulation results of route acquisition latency for variant number nodes considered in the range of 50 to 500 for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2].

Table 5: Tabulation for route acquisition latency

Number of nodes	Route acquisition latency (ms)		
	OLC-ROR	SRR	Anchor-based Routing
50	1.75	2.75	3.75
100	2.25	3.15	5.25
150	2.45	3.35	6.15
200	3.15	3.85	6.35
250	3.35	4.15	6.55
300	3.55	4.55	7.15
350	3.85	5.35	8.35
400	4.35	5.55	8.85
450	4.55	5.95	9.15
500	5.25	6.25	9.55

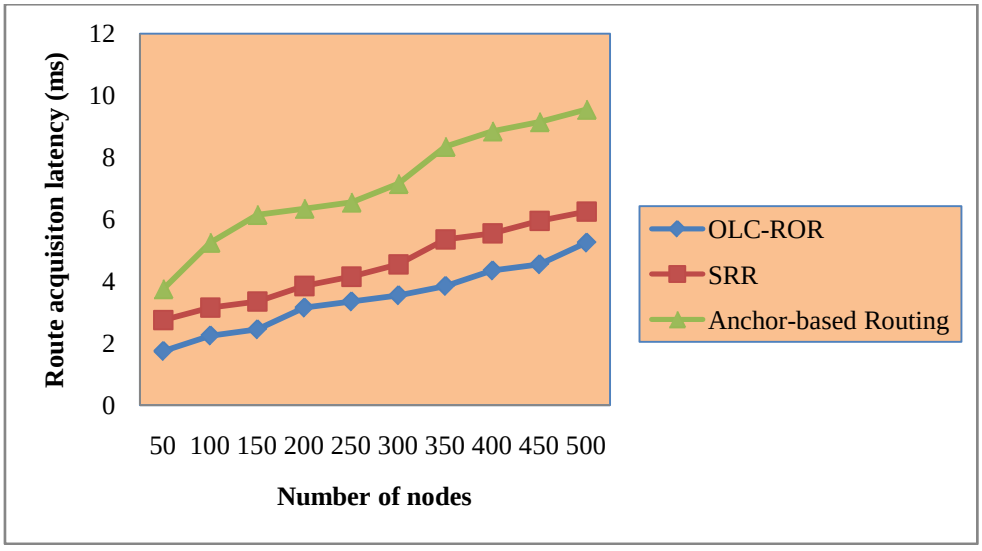


Figure 5: Measure of route acquisition latency over number of nodes

Figure 5 given above shows the performance evaluation of route acquisition latency over different numbers of nodes in the range of 50 to 500 for ten different simulation runs conducted at different time intervals over a wide area of network sizing 1000m*1000m. From the figure it is evident that, with increasing number of nodes, different numbers of optimal routes have to be identified and hence higher the route acquisition latency. From the simulations conducted for 50 numbers of sensor nodes, an optimal route to the sink node is identified within 1.75ms using the proposed OLC-ROR method, 2.75ms when applying with the SRR [1] method and Anchor-based Routing [2] method respectively. Route acquisition latency is said to be reduced using the OLC-ROR method when compared to [1] and [2]. By applying this algorithm, both the secured route and the genuineness of the node is identified. Here, a secured route is obtained via the onion route, and genuineness of the intermediate node is verified via the Rabin signature. Therefore, optimal and secured routes are obtained and with which the data packets are forwarded, minimizing the route acquisition latency using the OLC-ROR method by 24% compared to [1] and 52% compared to [2] respectively.

c) Performance measure of through put

Throughput refers to the average number of data packets successfully received per second to the number of data packets sent is given by

$$TP = \frac{DP_{rec}}{DPT_{sent}} \quad (12)$$

From the above equation (12), the throughput rate TP is measured based on the data packets successfully received DP_{rec} and the data packets sent DPT_{sent} . It is measured in terms of percentage (%). The sample calculations for throughput using the proposed OLC-ROR method, existing SRR [1], and anchor-based routing [2] are given below.

Sample calculation for throughput

- Proposed OLD-ROR: With 25 number of data packets to be sent and 22 number of data packets received at the sink node, the overall throughput rate is measured as given below.

$$TP = \frac{22}{25} * 100 = 88\%$$

- Existing SRR [1]: With 25 number of data packets to be sent and 21 number of data packets received at the sink node, the overall throughput rate is measured as given below.

$$TP = \frac{21}{25} * 100 = 84\%$$

- Existing anchor-based routing [2]: With 25 number of data packets to be sent and 20 number of data packets received at the sink node, the overall throughput rate is measured as given below.

$$TP = \frac{20}{25} * 100 = 80\%$$

Table 6, given below, shows the tabulation results of throughput for variant number packets considered in the range of 25 to 250 for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2].

Table 6: Tabulation for throughput

Number of data packets	Throughput (kbps)		
	OLC-ROR	SRR	Anchor-based Routing
25	88	84	80
50	85.35	82.15	79.35
75	81.25	80.45	78.15
100	80.35	77.15	77.55
125	80.25	75.35	73.25
150	80.15	74.25	72.15
175	78.25	71.55	65.35
200	75.35	70.35	64.15
225	75.55	70.15	62.25
250	75.15	68.45	60.3

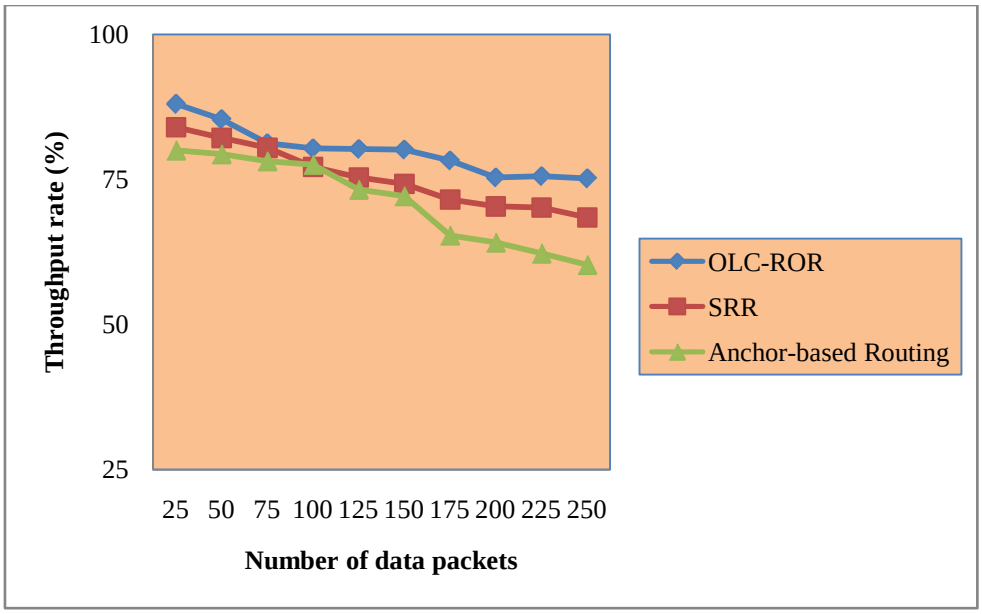


Figure 6: Measure of throughput over number of data packets

Figure 6, given above, shows the graphical representation of throughput rate. The figure x-axis refers to the number of data packets considered for experimentation, and the y-axis refers to the throughput rate. Here, the data packets considered for experimentation differ in the range of 25 to 250, with the packet size being 512 bytes for a maximum node speed of 20 km/hr spreading over a radio range of 250 m. From the figure, it is illustrative that the rate of throughput decreases with the increase in the number of data packets. As a result of that, with the increase in the number of data packets to be sent to the sink node specified for a stipulated destination node, the number of intermediate nodes in the network increases, and therefore the throughput rate reduces. However, from the simulation it is evident that with 25 number of data packets to be sent, the number of data packets received at the sink node using OLC-ROR method was found to be 22, 21 number of data packets received at the sink node using SRR [1] and 20 number of data packets received at the sink node using anchor-based routing [2]. From this, it is inferred that the throughput rate is found to be higher using the OLC-ROR method because of the application of Rabin signature and Onion routing. With this, anonymous communication over a computer network is said to be ensured. As a result of that, the nodes are encapsulated in layers, and the encrypted data is transmitted via a series of relay nodes called onion routers, uncovering the data's next destination. In this manner, security for the node carrying the data packets is said to be ensured. Besides, genuineness of the nodes in onion routers is established by applying the Rabin signature following random padding. In this way, throughput is said to be improved using the OLC-ROR method by 6% compared to [1] and 13% compared to [2], respectively.

VI. Conclusion

In this paper, we present a secured routing in Wireless Sensor Network (WSN) for the Internet of Things (IoT) using the Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method. The main aim is to improve the throughput rate and minimizes the routing overhead and route acquisition latency. Most of the optimal routing mechanisms focus on the energy consumption aspect and adopt the source location privacy and clustering for data routing. As a result, such solutions are non-feasible in dynamic scenarios where security plays a major role in routing. The proposed method designs a method that not only reduces the routing overhead and route acquisition latency but also improves the throughput rate, ensuring security in a significant manner. First, optimal route identification was made by determining the route possessing minimum load centroid and the residual energy, therefore reducing routing overhead. Next, the optimized secured routes were identified based on Onion routers using encapsulation, which reducing the route acquisition latency. Furthermore, the proposed method concentrated on the genuineness of the node that was ready to be routed using a Rabin signature, which ensured the throughput rate and therefore forming security. Simulation results have shown the OLC-ROR method effectiveness in securing the IoT network route as well as its low routing overhead and route acquisition latency with higher throughput.

References Références Referencias

1. Yu He, Guangjie Han, Hao Wanga, James Adu Ansere, Whenbo Zhang, "A sector-based random routing scheme for protecting the sourcelocation privacy in WSNs for the Internet of Things", Future

Generation Computer Systems, Elsevier, Feb 2019 [Sector-based Random Routing (SRR) method]
2. Catalina Aranzazu-Suescun and Mihaela Cardei, "Anchor-based routing protocol with dynamic clustering for Internet of Things WSNs", EURASIP Journal on Wireless Communications and Networking, Springer, Jul 2019
3. Hao Wang, Guangjie Han, Lina Zhou, James Adu Ansere, Wenbo Zhang, "A Source Location Privacy Protection Scheme Based on Ring-loop Routing for the IoT", Computer Networks, Elsevier, Nov 2018
4. Arezou Ostad-Sharif, Hamed Arshad, Morteza Nikooghadam, Dariush Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme", Future Generation Computer Systems, Elsevier, May 2019
5. Ilhem Souissi, Nadia Ben Azzouna, Lamjed Ben Said, "A multi-level study of information trust models in WSN-assisted IoT", Computer Networks, Elsevier, Jul 2019.
6. Jai Kumar Vinayagam, C.H. Balaswamy, K. Soundararajan, "Cross-layered-based adaptive secured routing and data transmission in MANET", International Journal of Mobile Network Design and Innovation, Vol. 9, No. 1, 2019, Inderscience
7. Hongsong Chen, Caixia Meng, Zhiguang Shan, Zhongchuan Fu,Bharat K. Bhargava, "A Novel Low-Rate Denial of Service Attack Detection Approach in Zig Bee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation", Security and Privacy For Cloud and IoT, IEEE Access, Mar 2019.
8. Shiju Sathyadevan, Krishnashree Achuthan, Robin Doss, Lei PAN," Protean Authentication Scheme A Time-Bound Dynamic Key Gen Authentication Technique for IoT Edge Nodes in Outdoor Deployments", IEEE, Jul 2019.
9. Turki Ali Alghamdi, "Convolutional technique for enhancing security in wireless sensor networks against malicious nodes", Human-centric Computing and Information Sciences, Springer, Jul 2019.
10. Ismail Butun, Patrik O sterberg, Houbing Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures", IEEE Communications Surveys & Tutorials, Oct 2019.
11. Yaw-Wen Kuo, Cho-Long Li, Jheng-Han Jhang, and Sam Lin, "Design of a wireless sensor network based IoTplatform for wide area and hetero generous applications", IEEE Sensors Journal (Volume: 18, Issue: 12, June15, 15 2018).
12. Geetha D. Devanagavi, N. Nalini and Rajashekhar C. Biradar, "Secured routing in wireless sensor networks using fault-free and trusted nodes", International Journal of Communication Systems, Wiley Online Library, Oct 2014.
13. Ming Luo, Yi Luo, Yuwei Wan, and Ze Wang, "Secure and Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT", Security and Communication Networks, Wiley, Feb 2018
14. Deebak B D, Fadi Al-Turjman, "A Hybrid Secure Routing and Monitoring Mechanism in IoT-based Wireless Sensor Networks", Ad Hoc Networks, Elsevier, Oct 2019
15. Travis Mick, Reza Tourani, Satyajayant Misra, "LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities", IEEE Internet of Things Journal (Volume: 5, Issue: 2, April 2018)
16. Khalid Haseeb, Naveed Islam, Ahmad Almogren, Ikram Ud Din, Hisham N. Almajed, Nadra Guizani, "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs", Mobile Edge Computing and Mobile Cloud Computing: Addressing Heterogeneity and Energy Issues of Compute and Network Resources, IEEE Access, May 2019
17. Catalina Aranzazu Suescun and Mihaela Cardei," Anchor-based routing protocol withdynamic clustering for Internet of Things WSNs", EURASIP Journal on Wireless Communications and Networking, Springer, Jul 2019
18. Imad Jawhar, Nader Mohamed, Jameela Al-Jaroodi, "Networking architectures and protocols for smart city systems", Journal of Internet Services and Applications, Springer, Jan 2018
19. Ramesh Sekaran and Ganesh Kumar Parasuraman, "A Secure 3-Way Routing Protocols for Intermittently Connected Mobile Ad Hoc Networks", Hindawi Publishing Corporation, The Scientific World Journal, Jul 2014
20. Songxiang Yang, Lin Ma, Shuang Jia, Danyang Qin, "A Novel Markov Model-Based Low-Power and Secure Multihop Routing Mechanism", Journal of Sensors, Hindawi, Oct 2019

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 2 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Anomaly Intrusion Detection based on Concept Drift

By Pradheep D, Gokul R, Naveen V & Vijayarani J
Anna University

Abstract- Nowadays, security on the internet is a vital issue and therefore, intrusion detection is one of the major research problems for networks that defend external attacks. Intrusion detection is a new approach for providing security in existing computers and data networks. An Intrusion Detection System is a software application that monitors the system for malicious activities and unauthorized access to the system. An easy accessibility condition causes computer networks vulnerable against the attack and several threats from attackers. Intrusion Detection System is used to analyze a network of interconnected systems for avoiding uncommon intrusion or chaos. The intrusion detection problem is becoming a challenging task due to the increase in computer networks since the increased connectivity of computer systems gives access to all and makes it easier for hackers to avoid their traces and identification. The goal of intrusion detection is to identify unauthorized use, misuse and abuse of computer systems. This project focuses on algorithms: (i) Concept Drift based ensemble Incremental Learning approach for anomaly intrusion detection, and (ii) Diversity and Transfer-based Ensemble Learning. These are highly ranked anomaly detection models. We study and compare both learning models. The Network Security Laboratory-Knowledge Discovery and Data Mining (NSL-KDD99) dataset have been used for training and to detect the misuse activities.

GJCST-E Classification: *J.7*

Strictly as per the compliance and regulations of:

Anomaly Intrusion Detection based on Concept Drift

Pradheep D[α], Gokul R[σ], Naveen V[ρ] & Vijayarani J[ω]

Abstract- Nowadays, security on the internet is a vital issue and therefore, intrusion detection is one of the major research problems for networks that defend external attacks. Intrusion detection is a new approach for providing security in existing computers and data networks. An Intrusion Detection System is a software application that monitors the system for malicious activities and unauthorized access to the system. An easy accessibility condition causes computer networks vulnerable against the attack and several threats from attackers. Intrusion Detection System is used to analyze a network of interconnected systems for avoiding uncommon intrusion or chaos. The intrusion detection problem is becoming a challenging task due to the increase in computer networks since the increased connectivity of computer systems gives access to all and makes it easier for hackers to avoid their traces and identification. The goal of intrusion detection is to identify unauthorized use, misuse and abuse of computer systems. This project focuses on algorithms: (i) Concept Drift based ensemble Incremental Learning approach for anomaly intrusion detection, and (ii) Diversity and Transfer-based Ensemble Learning. These are highly ranked anomaly detection models. We study and compare both learning models. The Network Security Laboratory-Knowledge Discovery and Data Mining (NSL-KDD99) dataset have been used for training and to detect the misuse activities.

I. Introduction

The Internet has a number of challenges to make it a secure system as it has a large amount of data and information. Computer networks are widely used by businesses, industries and various fields of day to day activity. Advances in technology and business, forced organizations and institutions worldwide to invent and use modern networks for safety. There are many types of attacks threatening computer networks. Dynamic mechanisms can be exploited though security can be ensured through the installation of firewalls and defending software. An intrusion detection system is one of the dynamic mechanisms that determines the specific goal of detecting attacks. An intrusion detection system (IDS) is one of the implemented solutions against hackers and attackers. Moreover, attackers always keep changing their techniques and tools for hacking the network. Intrusion detection system monitors the network and analyzes them to detect any kind of abnormalities, which are harmfull to computer security. There are two methods of intrusion detection (i) Misuse (ii) Anomaly.

A misuse detection system uses recognized patterns for detection, which is also called signature-based detection. A key benefit of these systems is that the patterns or signatures can easily develop and understand the network behavior, if familiar. Misuse aims to determine the attack signatures in the monitored resource. This technique is effective at detecting attacks that are already known. The time taken to match with the patterns stored in the database is minimal. Anomaly detection systems rely on constructing a model of user behavior that is considered normal. The detection of novel attacks is more successful using the anomaly detection approach for an intrusion. This is achieved by using machine learning methods to examine network traffic. Anomaly depends on knowledge of normal behavior and any deviation from normal behavior. Anomaly detection has gained popularity as it became effective against new anomaly attacks.

Concept drift is a change in the characteristics of the data stream. It means that the characteristics of the decision attributes and of the classes to be predicted, change in time in an unpredictable manner is called as concept drift. Such a situation may cause a decrease in classification quality and degrade learning mechanisms. Concept drift in machine learning refers to the change in the relationships between input and output data in the given data stream. A concept in “concept drift” refers to the unknown and hidden relationship between inputs and output variables. The change to the data could take any form. Some other types of changes may include (i) a gradual change over time, (ii) a recurring or cyclical change, (iii) a sudden or abrupt change.

The learning models need to adapt to the changes quickly and accurately. The concept drift detection technique is applied for autonomous detection of incoming new traffic. The drift detector could be recognized as the simplest classifier, but it is not as simple as it looks like. The drift detection can replace the outdated models and reduce time, but on the other hand, it should not accept too many false alarms. Concept drift detector is an algorithm that detects the information about incoming signal and return signals about its changing patterns. Usually, after returning the signal about the drift, the model should be rebuilt as quickly as possible.

Author α σ ρ: Final year B.E, Department of CSE, Anna University, Chennai. e-mail: duripradheep@gmail.com
Author ω: Teaching Fellow, Department of CSE, Anna University Chennai.

The ability of a classifier to take on new information and evolving the classifier without retrained on the data set fully is known as incremental learning. Incremental learning has been successfully implemented for many problems, where the data is changing. The goal of incremental learning is learning new training samples to improve the classification quality. There are many incremental learning models used for changing data, but various challenges arise in those learning mechanisms. Support vector machines, ensemble method and clustering are commonly used for incremental learning. In this paper, we used ensemble incremental learning model such as hierarchical Bayesian parameter estimation of the drift diffusion model (HDDM) as the drift detector.

Transfer learning is a machine learning method where a model developed for a task is reused as the starting point for a model to be applied on a second or another task. A pre-trained source model is chosen from available models. It is a popular approach where pre-trained models are used to solve tasks of other models. The model must be better than a naive or existing models to ensure that some feature learning has been performed and the model fits on the source task can then be used as the starting point for another model.

II. Realted Work

Pavl et al. (2005) developed an experimental framework for the analysis and comparison of supervised (classification) and unsupervised learning (clustering) techniques for detecting malicious activities in the net-work. The supervised methods evaluated in their work include support vector machines, multilayer perceptron, k-nearest neighbor, and decision trees. The unsupervised algorithms include k-means clustering and single linkage clustering. They assumed that training and test data come from the same unknown distribution and they consider the case where the test data comes from new attack patterns. This scenario helps us understand how much an IDS can adapt its knowledge to new malicious patterns. This is often very essential for an IDS system. The results showed that the supervised algorithms show better classification accuracy with known attacks on the data. Among these algorithms, the decision tree algorithm had achieved the best results. However, if there are unseen attacks in the test data, then the detection rate of supervised methods decreases significantly. This is where the unsupervised techniques perform better as they do not show a significant difference in accuracy for seen and unseen attacks. The supervised techniques generally perform better compared to unsupervised methods.

Tavallaee et al. (2009) analyzed the entire KDD data set statistically and made a re-port of it. The analysis showed that there are two important issues in the data set which highly affect the performance of evaluated systems, and results in a very poor evaluation of anomaly detection approaches. The issues are redundant records and level of difficulty. To solve these issues, a new data set, NSL-KDD which consists of selected records of the complete KDD data set was proposed. The number of records in the train and test sets is reasonable, which makes it perfect to run the experiments on the complete set without the need to randomly select a small portion. Therefore, the evaluation results of different research works will be consistent. There were no duplicate records in the proposed test sets; therefore, the performance of the learners is not biased by the methods which have better detection rates on the frequent records. NSL-KDD is a data set that was suggested to solve some of the inherent problems of the KDD'99 data set. Although this new version of the KDD data set still suffers from some of the problems and may not be a perfect representative of existing real networks, because of the lack of public datasets for network-based IDSs. Furthermore, the number of records in the NSL-KDD train and test sets is reasonable. This advantage makes it affordable to run the experiments on the complete set without the need to randomly select a small portion. Evaluation results of different research work can be consistent and used to be a comparable one.

Zamani and Movahedi (2013) suggested that traditional intrusion detection and prevention techniques, like firewalls, access control mechanisms, and encryptions, have several limitations. Protecting networks and systems from increasingly complex attacks like denial of service are hard for existing IDS. Most of the systems built based on such techniques suffer from high false negative and false positive detection rates and the lack of continuously adapting to changing behaviors. In this paper, they divided the ML-based approaches to intrusion detection into two categories: approaches based on artificial intelligence (AI) techniques and approaches based on Computational Intelligence (CI) methods. Important CI methodologies are artificial neural networks, evolutionary computation, artificial immune systems, and fuzzy logic. The unsupervised algorithms include the k-means clustering and single linkage clustering. Both supervised and unsupervised learning is used in Artificial Intelligence techniques. They reviewed several influential algorithms for intrusion detection based on various machine learning techniques.

Biswas (2018) proposed a system in which a subset of features is selected using feature selection algorithms and then the set of selected features is used to train different types of classifiers. They proposed an IDS model that compares the performances of different combinations of classifiers and feature selection algorithm. The feature selection techniques are CFS, IGR, PCA, and minimum redundancy. Maximum-relevance and the classifiers are k-NN, DT, NN, SVM,

and NB used in this paper. It is difficult to choose one algorithm or the classifier over another to implement an intrusion detection system. He used a different mix of feature selection algorithms and classifiers because each of the classifiers and the feature selection algorithms have an advantage as well as disadvantages. The highest accuracy obtained in all the combinations is for IGR feature selection with k-NN. k-NN classifier produces better performance than others. The IGR feature selection method is better than the others.

Yuan et al. (2018) proposed a network intrusion detection approach combining concept drift detection and incremental learning. They performed various machine learning mechanisms for intrusion detection and proposed a new learning method called concept drift ensemble incremental learning. Three classifiers are used and then they are ensemble into one. They used a hierarchical Bayesian parameter estimation of the Drift Diffusion Model method based on Hoeffding inequality as a concept drift detector to detect an abnormality and then designed ensemble-based incremental learning for classification. They used KDD CUP 99 set data set to demonstrate the robustness of the intrusion detection approach. They compared the normal incremental learning with the concept drift ensemble incremental learning and recorded the findings. They proved that concept drift ensemble incremental learning have higher accuracy than traditional incremental learning.

Sun et al. (2018) suggested a new ensemble learning approach, namely, DTEL, for incremental learning with concept drift. Diversity and Transfer-based Ensemble Learning employs a diversity-based selection to preserve previously trained models. A pre-trained model was used for retraining the selected features instead of directly applied to all features. The preserved or pre-trained models were further adapted to the current concept through transfer learning. The main potential drawback of DTEL is more costly than the other methods. Despite this disadvantage could be minimized by parallel implementation of DTEL since it can be naturally parallelized, it is still worth investigating other methods to reduce the complexity of DTEL. Other base learners were investigated to compare with DTEL. They used this algorithm on several data set like Cover type, poker hand, electricity, CTR Prediction. The accuracy of the other algorithms was compared with DTEL and proved its superiority.

III. System Design

a) System Architecture

The system (Figure 1) takes the NSL-KDD data set for pre-processing. The pre-processing involves mapping, feature scaling, data clearing, encoding, data sampling, and feature selection. Finally, the selected feature is mapped to the data set and the data set is split for training and testing. The drift is detected using the HDDM and Hoeffding tree algorithm. Incremental ensemble learning uses three classifiers such as MLP classifier, Multinomial NB and SGD classifier for training. In transfer learning, the model is trained with features and saved. The pre-trained model is again used for training and performance is measured with the first model.

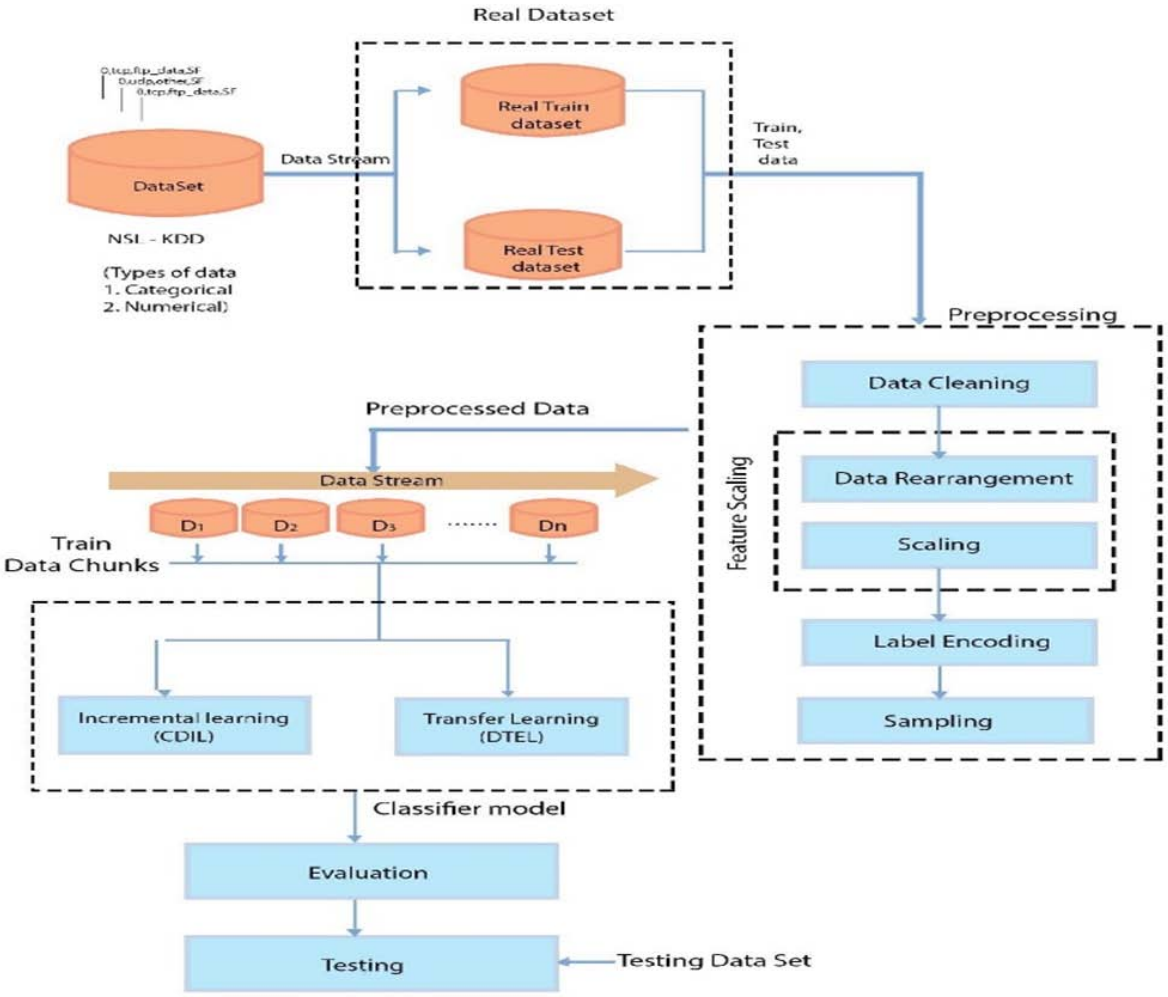


Figure 1: System Architecture

b) Data Processing

The data set is imported as a text document and then preprocessed. In preprocessing the data set is labeled and unwanted data columns are cleaned (Figure 2). The real data set which contains numerical data are scaled and characteristic data are encoded. The data set is sampled. It is followed by the feature selection process. In feature selection, only a few features are selected for training. After that, those features are mapped to the data set and other features are neglected. This proceeds with incremental and transfer learning.

c) Modules

i. *Data Processing*

First, the data set is labeled with the header and unwanted data columns with no values (i.e. fully occupied with zero) are dropped. The data set contains both numerical and characteristic data. The numerical data are scaled and character data are encoded. The data set is sampled for proper training. After sampling is done, it is followed by the feature selection process. In the feature selection process, only a few features that have a high influence on the target are selected for training.

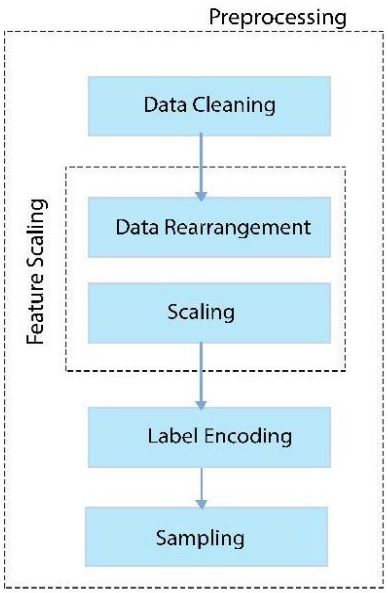


Figure 2: Data Processing

ii. *Incremental Learning (CDIL)*

Ensemble Incremental learning (Figure 3) helps to improve machine learning results by combining several models. Incremental learning keeps updating the model to generalize the model so that it doesn't deviate from the soul problem. Incremental learning is a machine learning mechanism where the learning process takes place whenever new examples or new attributes (attribute values) merge or deleted from the dataset and the solutions already obtained are only modified.

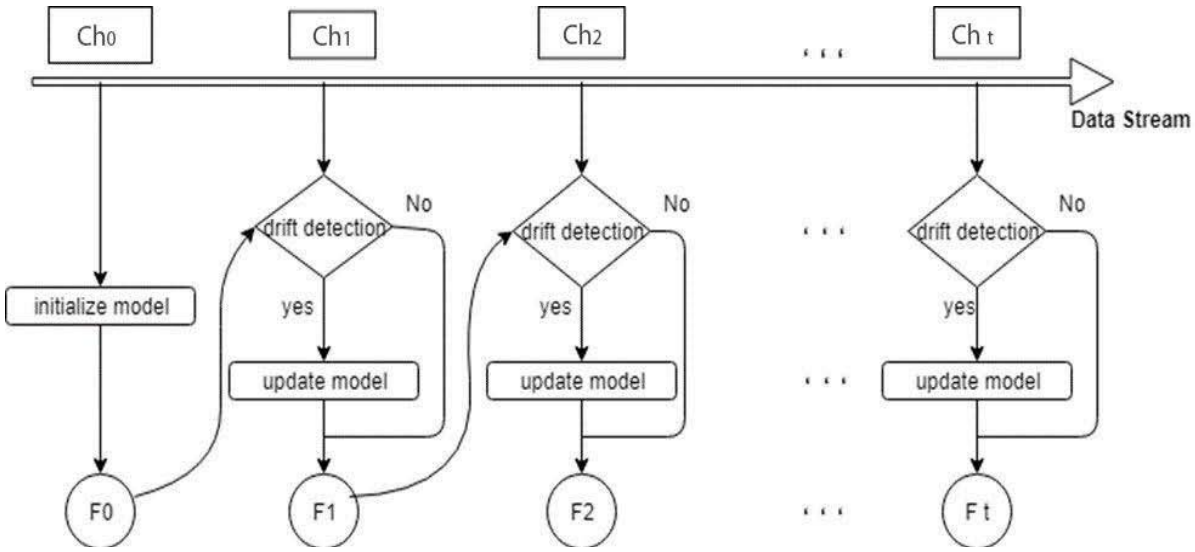


Figure 3: Incremental Learning

iii. *Transfer Learning*

The framework of transfer learning (Figure 4) differs from the other ensemble methods for incremental learning. First, it does not directly combine the outputs of historical models. Instead, each preserved historical model is first adapted to fit the current data, and then the adapted models and the model constructed from scratch are combined. This enables to achieve higher accuracy than the traditional method.

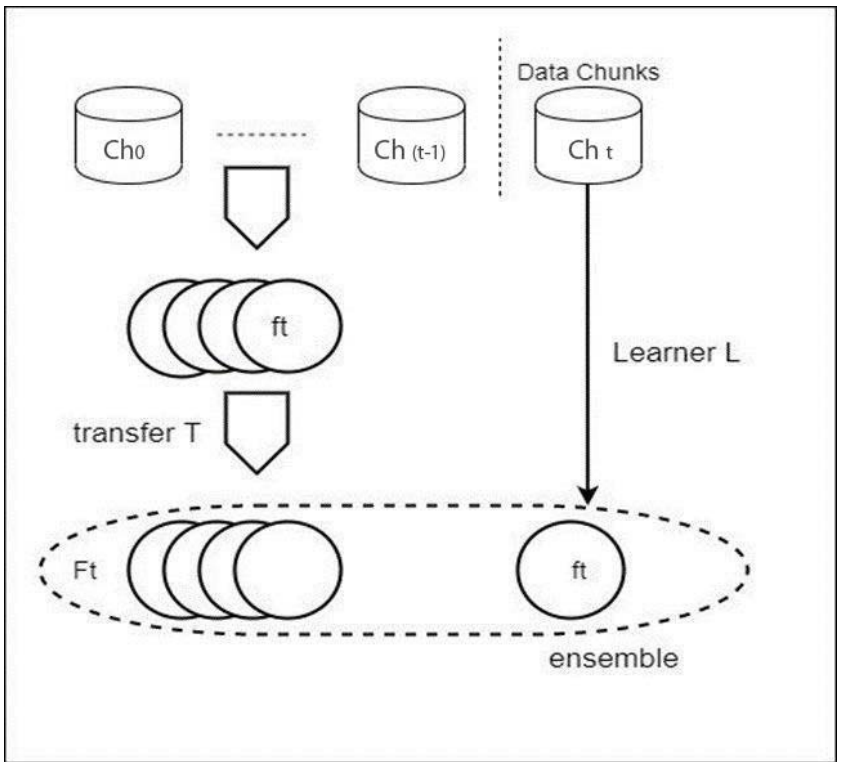


Figure 4: Transfer Learning

IV. System Development

a) Preprocessing

Large-scale data sets usually contain noisy, redundant and different types of data that present critical challenges to knowledge discovery and data modeling. Generally, the intrusion detection algorithms deal with one or more of the raw input data as numerical data only. Hence, we prepare data and convert categorical data in the dataset to numerical data. We found two important issues which highly affect the performance of evaluated systems, and results in a very poor evaluation of anomaly detection approaches. To solve these issues, we used the dataset NSL-KDD, which consists of the selected records of the complete KDD data set and does not suffer from any of mentioned shortcomings.

i. *Mapping*

The attacks in the data set were classified into 4 groups based on the data used by Tavallaee et al (2009). They are classified as Dos, R2L, Probe and U2R. But the dataset contains the attack as differentiated into 21 types of vulnerabilities. Hence, mapping in python is used to match all the attacks into five categories.

ii. *Scaling numerical attribute*

In machine learning, standardization is a key technique to get reliable results. Values for some features may diverge from small to very big numbers and the processes analyzed may explode the scale. Thus, all the values are scaled to a range.

iii. *Encoding*

We used the label encoding. In label encoding, we map each category to a number or a label. The labels chosen for the categories have no relationship. So categories are close to each other and lose such information after encoding.

iv. *Sampling*

Data sampling refers to statistical methods for selecting observations from the domain with the objective of estimating a population parameter. Data sampling is used to balance the data set. The recursive feature elimination is used to select the important feature with a high correlation.

v. *Feature selection*

Feature selection is the process of selecting a subset of relevant features (variables, predictors) for use in model construction. We have 40 features in the data set hence we reduce them to nine features because it enables the machine learning algorithm to train faster. It reduces the complexity of a model and makes it easier to interpret.

b) Incremental learning

Algorithm 1:

Input: Preprocessed Data set

Output: Incremental model

1: from classifier.import hoeffding tree
2: from drift-detection.import hddm
3: Labels = Selected feature labels
4: Attributes = Selected feature attributes
5: Pairs = Hoeffding tree, hddm
6: Drift points = 20000, 40000, 60000, 80000
7: Acceptance interval = 250
8: Detection = Evaluate(Hoeffding tree, hddm, drift points, acceptance interval)

Algorithm 2:

Input: Data Chunk

Output: Drift Detected in data stream.

1: hddm (data set)
2: for i= length of data set do
3: Perform detection
4: if (detects drift point) then
5: Perform detection on next set
6: if (detects drift point) then
7: Update the model
8: else
9: Discard
10: end if
11: end if
12: end

c) Transfer learning

The model is trained with sequential classifier and then it is re-trained for n times.

Input: Preprocessed Data Set

Output: Classifier for data set

Algorithm:

1: from keras.models import Sequential
2: model= add (feature=n, hidden layer = k)
3: model= add (hidden layer = k-4)
4: Data set = model fit
5: Save the model
6: for i= fixed length do
7: for a = range of evaluation do
8: Load saved model
9: Retrain model (a)
10: end
11: end
12: evaluate

V. Results

This project used NSL-KDD data set which contains over 130000 data for training and 12000 data for testing.

In this paper, we first analyzed the dataset and plotted the distribution of the attack class (Figure 5). It gives a clear view of attack class distribution in both train and test data. The unwanted data are dropped. After this, we scaled the integer data into float and then the characteristic attributes into the integer. Because, machine learning can't be performed on the character data.

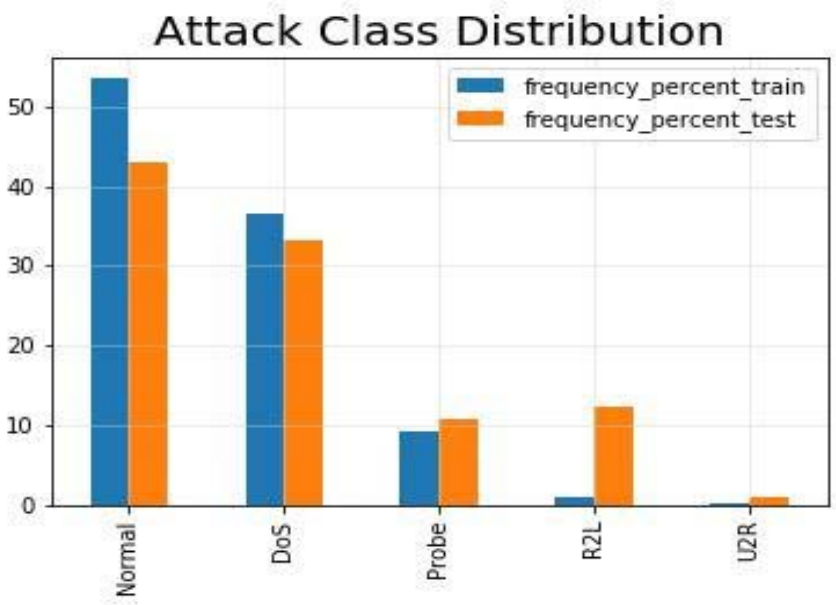


Figure 5: Attack Class Distribution

From this graph, we understand that, attack classes in test data is higher than the train data. This may affect learning. Hence, sampling is done and followed by feature selection. Feature selection is performed by the random forest classifier which sorts the features and it is plotted (Figure 6).

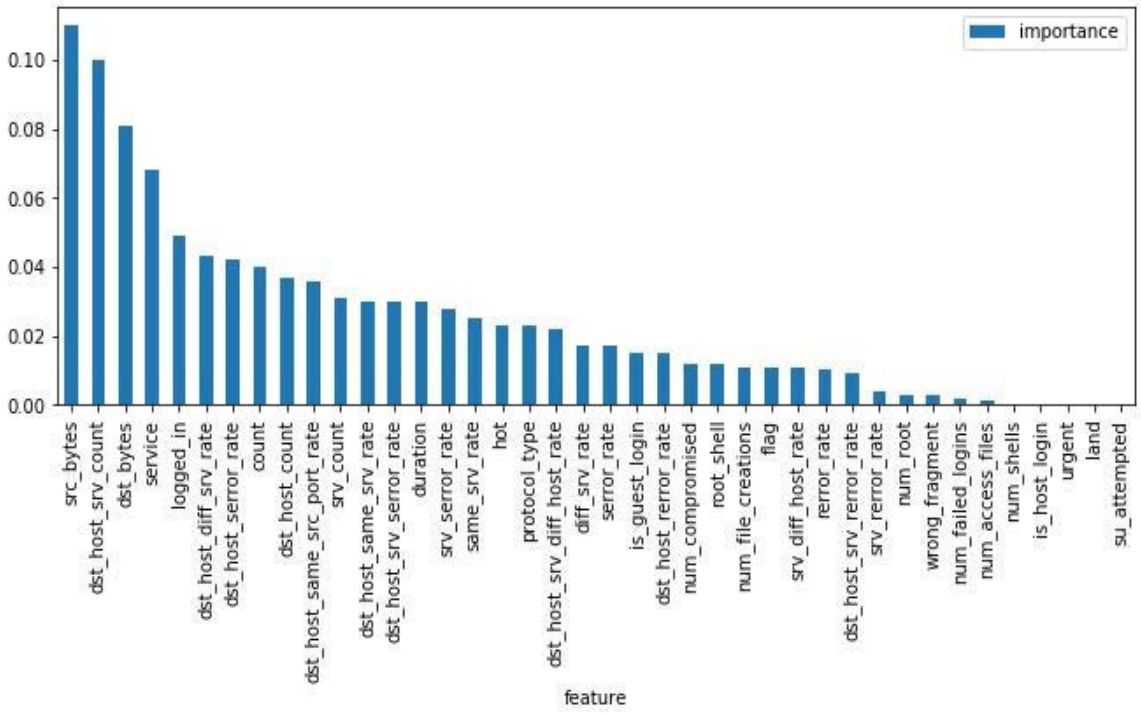


Figure 6: Features with high priority

From these first 10 features which have high priority is selected and those features are sorted in both train and test data set.

The drift is detected using the HDDM and Hoeffding tree algorithm. The peak points show the drift in the concept (Figure 7).

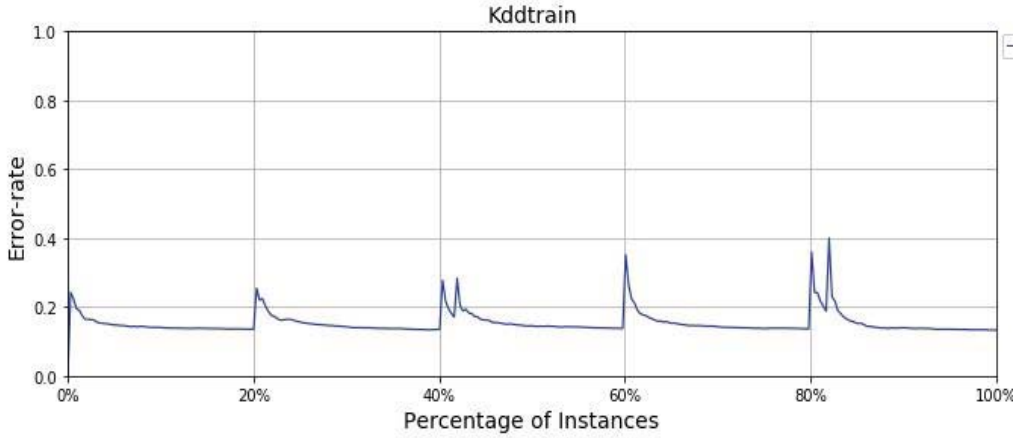


Figure 7: Drift Detection

Then in incremental ensemble learning classifiers such as MLP classifier, Multinomial NB and SGD classifier are used for training. The cross validation score is a statistical method used to estimate the performance of machine learning models. It is commonly used in machine learning to compare and select a model for a given predictive modeling problem because it is easy to understand and easy to implement. The cross-validation score is 0.880434910 which is +/- 0.003 of accuracy and shows that there is no overfitting.

Transfer learning makes use of the knowledge gained while solving one problem and applying it to a different but related problem. The knowledge of an already trained machine learning model is applied to related problem.

Table 1: Accuracy Analysis

	Incremental Learning	Transfer Learning
Accuracy	0.79%	0.88%

Higher accuracy is achieved with the transfer learning model (Table 1).

VI. Conclusion

In this paper, HDDM method is used based on Hoeffding inequality as a concept drift detector to detect an abnormality in the data chunks and then three classifiers are used to classify the intrusion. The transfer learning mechanism used in the proposed model shows higher accuracy than the incremental learning. The transfer learning used the knowledge from the previous learning and used it in the subsequent learning iteration. The evaluation results based on the NSL-KDD dataset demonstrate the intrusion detection approach. Hence the transfer learning can also be used in the intrusion detection system which contains sudden or abrupt concept drift.

References Références Referencias

1. Biswas, Saroj Kr. "Intrusion detection using machine learning: A comparison study." International Journal of Pure and Applied Mathematics 118, no. 19 (2018): 101-114.
2. Laskov, Pavel, Patrick Düssel, Christin Schäfer, and Konrad Rieck. "Learning intrusion detection: supervised or unsupervised?." In International Conference on Image Analysis and Processing, pp. 50-57. Springer, Berlin, Heidelberg, 2005.
3. Sun, Yu, Ke Tang, Zexuan Zhu, and Xin Yao. "Concept drift adaptation by exploiting historical knowledge." IEEE transactions on neural networks and learning systems 29, no. 10 (2018): 4822-4832.
4. Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6. IEEE, 2009.
5. Yuan, Xiaoming, Ran Wang, Yi Zhuang, Kun Zhu, and Jie Hao. "A Concept Drift Based Ensemble Incremental Learning Approach for Intrusion Detection." In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 350-357. IEEE, 2018.
6. Zamani, Mahdi, and Mahnush Movahedi. "Machine learning techniques for intrusion detection." arXiv preprint arXiv: 1312.2177 (2013).

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 2 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

ERP Security Based on Web Services

By Mamoun Hadidi & Saleh Hadidi

Abstract- The ERP system is one of the most important systems implemented by organizations in Jordan, whether governmental or private organizations. Because of the numerous development in Internet services and the increasing dependence on web services, this has led to the appearance of many types of ERP systems that depend on web services and use the web interface as the main interface for the system, and because of this development in the ERP system and its dependence on web services, this has led to problems in security with ERP system, especially since this system will be vulnerable to a hacker attack because it contains important data for organizations because the ERP system is a large database that serves all departments of organizations such as the finance, administrative, and marketing departments. This makes it a major target through which hackers seek access to organization data, which makes the security of an ERP system based on Web services an important topic that must be studied. Therefore, this paper will focus on the topic of ERP Security and will address the basic principles, properties, main requirements, and challenges of ERP system security based on Web services.

GJCST-E Classification: *H.3.5*

Strictly as per the compliance and regulations of:

ERP Security Based on Web Services

Mamoun Hadidi [α] & Saleh Hadidi [σ]

Abstract- The ERP system is one of the most important systems implemented by organizations in Jordan, whether governmental or private organizations. Because of the numerous development in Internet services and the increasing dependence on web services, this has led to the appearance of many types of ERP systems that depend on web services and use the web interface as the main interface for the system, and because of this development in the ERP system and its dependence on web services, this has led to problems in security with ERP system, especially since this system will be vulnerable to a hacker attack because it contains important data for organizations because the ERP system is a large database that serves all departments of organizations such as the finance, administrative, and marketing departments. This makes it a major target through which hackers seek access to organization data, which makes the security of an ERP system based on Web services an important topic that must be studied. Therefore, this paper will focus on the topic of ERP Security and will address the basic principles, properties, main requirements, and challenges of ERP system security based on Web services.

I. Introduction

Organizations in the world are using a wide variety of information systems to Support their products and services to growing business and improve organizational performance (Al-Dhaafri et al, 2016).

ERP systems in large and medium-sized organizations contribute to the management and use of their resources (materials, human resources, financing, etc.) in effective ways, by providing integrated solutions to the organization's information processing needs. (Olson DL et al., 2012)

ERP systems are a key component of government or private organizations. The ERP system contains important data that is exposed to many threats both external and internal, has a significant impact on the failure of the Organization's work. Therefore, all security aspects such as Integrity, confidentiality and availability are critical in the ERP system (Gupta et al., 2017).

The other important benefits of an ERP as following as:

- Lower operational cost by defined and more streamlined business processes (oracle, 2017).
- Improve efficiency Through a common user experience across many business functions and managed business processes (oracle, 2017)
- Integrate financial information: each organization need to understand the company's overall performance, organization find many different ways of calculate set of revenue numbers, and each department in the organization has its own contribution to the total profits of the organization calculated by ERP system.
- To standardize and speed up manufacturing processes Manufacturing companies especially those with a desire for mergers and acquisitions often find ways to mergers using different methods and computer systems (Wailgum &Thomas, 2017).
- ERP systems provide standard methods for automating phases of a manufacturing process. Standardizing those processes and using a single, integrated (Wailgum &Thomas, 2017).
- Organize human resource information: organizations that have multiple units prefer use ERP system to unify and tracking employee information that help organization to evaluate employee performance (Wailgum &Thomas, 2017).

II. Principles of ERP System Security based on Web Services

Security principles for system designers are considered as guidelines in the design and implementation of systems security.

There are many security principles will be mentioned as follows:

a) Security Defense in depth

This principle is based on the imposition of security policies on every layer of the system and the architecture of this system, which prevents the hacker from infiltrating the system (Kumar,2014). In addition, enterprises apply this principle by using the firewall as the first line of defense, the second line is using Web server security, the third line operating system security, database security level and other levels as the customer needs.

b) Patch the weakest link

This principle depends on the designers of the systems to identify weaknesses in the security of the system in various components by conducting tests of the system and try to penetrate this system (Kumar, 2014). Also strengthen any weak layer can be penetrated.

c) Classifications

This principle classifies all system resources and functions into different security classifications, limiting access to users with appropriate roles and

Author α σ: e-mails: hadidi2020@outlook.com, Saleh_hadidi2003@yahoo.com

privileges (Kumar, 2014). In addition to preventing accidental access to system confidential data and preventing unauthorized access to the system.

d) Single entrance point of entry

The ERP system should allow users only through a single authentication point and should avoid other points of entry and URL shortcuts. However, the importance of this principle reduces the chances of penetration to secret data and unauthorized access to data(Kumar,2014). It also has all the web pages protected and automatically redirected to the login page that performs as a single entry point. The system does not allow access to system data through pages other than the login page.

e) User data validation

The data inserted by the user should be validated and cleaned at various levels in the system. Data must also be properly encrypted when saved and transported into different layers (Kumar, 2014). However, the importance of this principle is to prevent attacks caused by the introduction of malicious contents into system data. The security mechanism checks the data entered by the user in the client layer and on the server layer using different verification methods.

III. Properties of ERP System Security based on Web Services

There are five security properties as follows (Messaoud and Diouri, 2014):

a) Confidentiality

This property includes preventing unauthorized persons from reading the information and allowing only those authorized to read the information from the system.

b) Integrity

This feature does not allow unauthorized users to allow modification of data in the system, and only allow modification of data to authorized users.

c) Authenticity

This property ensures that the person using the system is the same person who is allowed to use the system.

d) Non-repudiation

This property ensures that the appropriate proof is logged in the user transaction log so that the user is not allowed to deny the transaction.

e) Availability

This property ensures that users can access the information in the system at any time without any obstacles preventing this property.

IV. Security challenges of ERP System Security based on Web Services

ERP systems are of critical nature because of the value of the data they contain and the need to adopt the complete confidentiality of these data .also what may be dangerous to all department of the organization because of any security breach of data, representing security challenges is a real problem for organizations using the ERP system.

The main of the security challenges facing the ERP system is as follows:

1. Passwords are used in the default database or default applications.
2. Access to the system from outside the place of the organization using this system.
3. Direct access to the database system by users of this system inside the organization.
4. The bad design of the security system of the ERP system by the providers, which leads to security problems in this system.
5. Not using a data encryption system in the ERP system that prevents any data leaks during data transfers and update information.
6. Weak passwords and the inability to control them because of the use of many machine passwords.

V. Security Requirement of ERP System Security based on Web Services

Data-level transactions are performed securely from one end to the other during transport and data storage. Requirements for providing comprehensive security for web services are summarized in following table (Messaoud and Diouri, 2014):

Requirement	Clarifications
Authentication	There is an urgent need for the system to verify the identity of the user. Especially in the case of mutual authentication because users may have indirect contact with the system. Therefore, multiple authentication methods are used and can be grouped together. These methods include password and Lightweight directory access protocols (LDAP)
Authorization	Authorization: This requirement is necessary to control the process of authorizing access to information about the system, and determining the mechanisms of delegation for the system
Data Integrity and Data Confidentiality	Data integration technology guarantees that data has not been changed during the transmission process. This technique also includes data confidentiality using various encryption and digital signature technologies.
Audit Trails	This requirement includes the audit process and tracking user access and behaviour. In order to reduce the occurrence of any violations and check the accounts to ensure that this violation does not occur and repair any gap may lead to any violation

VI. Conclusions

This paper focused on ERP security based on web services where this study explained the ERP system in terms of its definition and indicated the extent of its importance for governmental and private organizations as this system is one of the most important systems that organizations seek to implement due to the great benefits that this system provides to organizations.

The implementation of the ERP based on web services faces many challenges and difficulties and the most important of these challenges, which this study focused on are security challenges, so the study clarified the basic principles upon which the security systems that used in ERP based on web services, where the study found that the most important safety principles that should be present are Security defence-in-depth, Patch the weakest link, Classifications, Single entrance point of entry and User data validation.

Also, the study explained the most important security characteristics of the ERP based on web services that must be contained in the security system, which are Non-repudiation, Authenticity, Confidentiality and Availability.

Nevertheless, the implementation of the ERP system faces many challenges, so the study explained the most important of these challenges that face the implementation of the system, and there are many requirements that the security application requires in the ERP system based on web services, so this study explained the most important system requirements that must exist In order to activate security with high efficiency, the most important of these requirements are Authentication, Authorization, Data Integrity, Audit Trails.

References Références Referencias

1. Al-Dhaafri, H. S. and Al-Swidi, A. (2016) 'The impact of total quality management and entrepreneurial orientation on organizational performance', International Journal of Quality and Reliability Management.
2. Farrington, R. et al. (2017) 'Oracle ® E-Business Suite', (August).
3. Gupta, S. et al. (2017) 'Identification of challenges and their ranking in the implementation of cloud ERP: A comparative study for SMEs and large organizations', International Journal of Quality and Reliability Management, 34(7), pp. 1056–1072. doi: 10.1108/IJQRM-09-2015-0133.
4. Houssain, E. et al. (2014) 'Web Service Security Overview, analysis and challenges', 11(5), pp. 124–139.
5. Kumar, SS 2014, Architecting High Performing, Scalable and Available Enterprise Web Applications, Elsevier Science & Technology, San Francisco. Available from: ProQuest Ebook Central. [8 February 2019].
6. Link, B. and Back, A. (2015) 'Classifying systemic differences between Software as a Service- and On-Premise-Enterprise Resource Planning', Journal of Enterprise Information Management, 28(6), pp. 808–837. doi: 10.1108/JEIM-07-2014-0069.
7. Olson DL, Van Huy V, Tuan NM. Case of development of a small business ERP consultant knowledge base. Advances in Enterprise Information Systems II 2012. p. 81.
8. Thomas, W. (2017) 'What is ERP? Definition and FAQs - ProQuest', ERP Systems, pp. 1–13. Available at: https://search-proquestcom.ezproxy.napier.ac.uk/docview/1919042734?rfr_id=info%3Axri%2Fsid%3Aprimo.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 2 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Internet of Things (IoT) for Agriculture Growth using Wireless Sensor Networks

By Rakesh Kumar Saini & Chandra Prakash
DIT University

Abstract- Farming productions are a necessary employment in industrial and for employment. The Internet of Things (IoT) has the capability to convert the methods we stay in the universal. We have additional-effective manufacturing, greater associated vehicles, and smoother townships, a lot of these as flavors of an integrated Internet of Things (IoT) system. Smooth agriculture via the usage of Internet of Things (IoT) technologies will help agriculturalists to minimize produced wilds and improve efficiency. That can come from the amount of compost that has been applied to the wide variability of expeditions the farm automobiles have complete. So, ingenious undeveloped is essentially a hello-tech device of emerging food this is horizontal and is maintainable for the crowds. The use of Information Technology (IT) and items like sensors, self-necessary automobiles, automatic hardware, operate constructions, automation, and so forth on this method are key instruments. In this paper we have a look at how agriculture fields are profited from Internet of Things constructions. We enclosed the detailed Internet of Things (IoT) Solicitations in Agriculture and the way they're functional. This paper provides an indication of the existing condition and future calculations of Internet of Things (IoT) solicitations in Agriculture.

Keywords: *IoT applications, smart cities, smart environment, smart farming, smart healthcare.*

GJCST-E Classification: *C.2.1*

Strictly as per the compliance and regulations of:

Internet of Things (IoT) for Agriculture Growth using Wireless Sensor Networks

Rakesh Kumar Saini [α] & Chandra Prakash [σ]

Abstract- Farming productions are a necessary employment in industrial and for employment. The Internet of Things (IoT) has the capability to convert the methods we stay in the universal. We have additional-effective manufacturing, greater associated vehicles, and smoother townships, a lot of these as flavors of an integrated Internet of Things (IoT) system. Smooth agriculture via the usage of Internet of Things (IoT) technologies will help agriculturalists to minimize produced wilds and improve efficiency. That can come from the amount of compost that has been applied to the wide variability of expeditions the farm automobiles have complete. So, ingenious undeveloped is essentially a hello-tech device of emerging food this is horizontal and is maintainable for the crowds. The use of Information Technology (IT) and items like sensors, self-necessary automobiles, automatic hardware, operate constructions, automation, and so forth on this method are key instruments. In this paper we have a look at how agriculture fields are profited from Internet of Things constructions. We enclosed the detailed Internet of Things (IoT) Solicitations in Agriculture and the way they're functional. This paper provides an indication of the existing condition and future calculations of Internet of Things (IoT) solicitations in Agriculture.

Keywords: IoT applications, smart cities, smart environment, smart farming, smart healthcare.

I. Introduction

Internet of Things (IoT) is a mechanism of computing strategies that are related from each dissimilar. These computing devices must be strength-strapped in addition to digital technologies and these computing devices can transmission Information over a network disadvantaged of disconcerting human-to-human or human-to-computer Oral conversation. Kevin Ashton, in a presentation of Procter & Gamble in 1999, invented the period "Internet of Things". Virtually each area, device, instrument, software, and so forth are related to respectively other. The forthcoming to admittance these devices through a phone or finished a computer is declared to as Internet of Things (IoT).These devices are recovered from are serve.

For example, an In-flight Conditioner's device container get the documentations concerning the out of doors hotness, and for this reason modify its hotness to prosperous or decrease it with esteem to the out of doors climate. Similarly, your freezers also can regulate its temperature thus. This is how devices can cooperate with a network. The entire system activates with the devices themselves, such as smart phones, effective watches, electronic home tools which strongly express with an internet of features platform. IoT stage gathers and associations figures from more than one devices and systems and applies analytics to amount the most valuable particulars with programs to contract with enterprise-particular necessities. Smart undeveloped is an often overlooked Internet of Things (IoT) reasonableness. However, outstanding to the component the amount of undeveloped processes is characteristically distant and the massive wide inconsistency of farmstead animals that agriculturalists effort on, all of this may be supervised with the support of the Internet of Things (IoT) and container also transform the manner agriculturalist's paintings. But this concept is butt attain a huge-scale interest. However, it still stays to be one of the Internet of Things (IoT) correspondences that should not be underestimated. Horizontal undeveloped has the probable to come to be a necessary software subject mostly in the agricultural-product spreading countries. The devices inside the Internet of Things (IoT) machine within the greenhouse offer numbers on infection, nervousness, humidity, light periods. The Internet of Things (IoT) technology has understood the smart wearable's, connected devices, automatic machines, and driverless automobiles. However, in farming, the Internet of Things (IoT) has presented the supreme result. With the arrival of Industrial IoT in Farming, a long way more larger sensors are being applied. The sensors are now connected to the cloud thru mobile/satellite TV for pc community. Which we could us to realize the actual-time information from the sensors, making decision making powerful. The programs of internet of Things (IoT) in the farming inventiveness has aided the agriculturalists to small screen the liquid container levels in real-time which makes the irrigation method additional well-ordered. The improvement of Internet of Things (IoT) generation in agriculture operations has added the use of sensors in each stage of the agriculture technique like how a lot time and properties a seed receipts to turn out to be a totally- full-grown plant. Smart Agriculture is a hello-tech and real means of accomplishment farming and growing food in a sustainable method. It is a usefulness of applying linked implements and inventive equipment cooperatively interested in farming.

Author α σ: School of Computing, DIT University, Dehradun Uttrakhand, India. e-mails: rakeshcool2008@gmail.com, chandra.prakash.19@gmail.com

Figure 1: Internet of Things for Agriculture

Smart Farming majorly depends on Internet of Things (IoT) as an importance casting off the need of biological landscapes of growers and cultivators and therefore growing the productivity in every attainable means. In this paper we look at the effect of IoT in agriculture.

II. Uses of Internet of Things

The main solicitations or purpose of IoT are summarize in table 1.

Table 1: Uses of Internet of Things (IoT)

Smooth Constructions	Applications switch and watching, Drive and Utility Organization, etc.
Smooth Metering	Air, Electrical, Water metering, introducing, fault detection and more.
Smart Towns	Transportation Organization, Bedside
	light, Liquid & Unwanted organization, etc.
Smart Homemade	Utilizations, room situation, watching, supervisory, etc.
Smart Farming	Water supply, Fertility, Yield and Disease management.
Oil and Gas Manufacturing	Metering, accountability discovery, isolated watching and regulatory.

III. Why Adopt IOT used for Agriculture

Solicitation of IoT in agriculture might be a life changer used for civilization and the whole earth. Currently, we observer how dangerous weather, flagging earth and drying parklands, fall down environments that play a crucial role in agriculture make food production harder and harder. Internet of Things (IoT) Technology will support agriculturalists to decrease produced wastelands and improve efficiency. That can originate from the amount of compost that has been applied to the number of missions the farmhouse automobiles have completed. So, smart agriculture is essentially an automated system of emerging nutrition that is uncontaminated and is supportable for the crowds. Internet of Things based Smooth Agricultural expands the complete Farming system by observing the ground in actual. With the help of devices and interconnectivity, the Internet of Things (IoT) in Farming has not individual saved the period of the agriculturalists but has also summary the wasteful use of properties such as Liquid and Power. It conserves frequent topographies like moisture, high temperature, soil etc. above checked and provides a crystal strong real- time surveillance. There are some benefits of adopting Internet of Things (IoT) for Agriculture:

a) Precision Farming

Precision farming is a manner or an exercise that makes the farming process greater correct and managed for raising live stock and growing of crops. The use of IT and items like sensors, self-sustaining automobiles, computerized hardware, control systems, robotics, and many others. In this technique are key additives. Precision agriculture inside the latest years has turn out to be one of the maximum well-known programs of IoT in agricultural area and a massive range of groups have started using this approach around the arena.

Figure 2: Precision farming using IoT

b) Data Analytics

The predictable database system does now not have enough garage for the facts amassed from the IoT sensors. Cloud primarily based facts garage and a stop-to-stop IoT Platform plays an important role in the clever agriculture machine. These systems are predicted to play an essential role such that higher sports can be finished. In the IoT world, sensors are the primary supply of amassing facts on a huge scale. The statistics is analyzed and transformed to meaningful facts the usage of analytics gear. The records analytics helps inside the evaluation of weather conditions, farm animals situations, and crop situations. The statistics amassed leverages the technological improvements and for this reason making better choices. With the help of the IoT devices, you may understand the real-time repute of the

plants with the aid of capturing the facts from sensors. Using predictive analytics, you may get a perception to make better decisions related to harvesting. The fashion analysis helps the farmers to recognize upcoming climate conditions and harvesting of vegetation. IoT in the Agriculture Industry has helped the farmers to maintain the quality of vegetation and fertility of the land, as a result improving the product volume and exceptional.

c) Climate Conditions

Climate plays a completely critical role for farming. And having mistaken know-how about climate closely deteriorates the amount and first-class of the crop production. But IoT answers permit you to know the real- time weather situations. Sensors are placed inside and outside of the agriculture fields. They gather statistics from the environment that is used to choose the proper plants which could develop and maintain within the precise climatic situations. The entire IoT atmosphere is made of sensors that can locate real-time climate conditions like humidity, rainfall, temperature and greater very correctly. There are numerous no of sensors to be had to hit upon a lot of these parameters and configure accordingly to fit your clever farming necessities. These sensors reveal the situation of the crops and the climate surrounding them. If any worrying climate conditions are determined, then an alert is ship. What receives removed is the want of the physical presence in the course of worrying climatic conditions which ultimately increases the productiveness and help farmers to acquire greater agriculture approvals.

d) Smart Greenhouse

Greenhouse farming is a technique that complements the yield of crops, greens, end result etc. Greenhouses manage environmental parameters in two ways; both through manual intervention or a proportional control mechanism. However, for the reason that manual intervention has dangers inclusive of production loss, energy loss, and labor price, these methods are much less effective. A smart greenhouse via IoT embedded structures now not simplest monitors intelligently but also controls the climate. There by disposing of any need for human intervention. Different sensors that degree the environmental parameters in step with the plant requirement are used for controlling the environment in a smart greenhouse. Then, a cloud server create for remotely having access to the machine while it associates the use of IoT. Confidential the greenhouse, the cloud server allows in the processing of records and applies a manage movement. This design offers best and value- powerful solutions to the farmers with minimum and nearly no manual intervention.

e) Agricultural Drones

Scientific advancements has nearly revolutionized the agricultural operations and the introduction of agricultural drones is the trending disruption. The Ground and Aerial drones are used for assessment of crop fitness, crop monitoring, planting, crop spraying, and field evaluation. With right strategy and planning based on actual-time facts, drone generation has given a high upward push and makeover to the agriculture industry. Drones with thermal or multi spectral sensors pick out the areas that require changes in irrigation. Once the plants begin developing, sensors imply their health and calculate their plants index. Eventually clever drones have decreased the environmental effect. The consequences were such that there has been a large reduction and much decrease chemical accomplishing the groundwater.

Figure 3: Smart farming using Drones

f) Livestock Monitoring

Internet of Things correspondences help agriculturalists to obtain material regarding the neighborhood, correctly- existence, and well-being in their livestock. This measurements permits them in recognizing the location of their livestock. Such as, finding animals that are unwell so, that they could break free the herd, preventing the unfold of the disease to the whole livestock. The feasibility of ranchers to find their farm animals with the help of Internet of Things (IoT) based sensors allows in transporting depressed hard work charges by a pronounced amount.

IV. Case Studies of IOT for Agriculture

There are some cases studies of IoT for agriculture grow are:

a) Monitoring of climate conditions

Probably the maximum famous smart agriculture devices are weather stations, combining diverse clever farming sensors. Located throughout the sector, they acquire numerous information from the environment and ship it to the cloud. The furnished measurements can be used to map the climate situations, choose the proper crops, and take the desired measures to improve their potential. Some

examples of such agriculture IoT devices are all METEO, Smart Elements, and Pycno.

Figure 4: Monitoring of climate conditions

b) Greenhouse automation

In addition to sourcing environmental information, weather stations can automatically modify the situations to fit the given parameters. Precisely, greenhouse automation structures use a similar precept. For instance, Farm app and Grow link are also IoT agriculture merchandise providing such competencies among others. Green IQ is likewise an interesting product that makes use of smart agriculture sensors. It is a smart sprinklers controller that permits you to perform your irrigation and lights systems remotely. A greenhouse farming technique complements the produce of vegetation by way of controlling environmental parameters. However, guide coping with effects in production loss, strength loss, and hard work fee, making the procedure much less effective. A conservatory with embedded gadgets not best makes it less complicated to be supervised however additionally, allows us to manipulate the temperature interior it. Sensors amount specific parameters in step with the plant requirement and ship it to the cloud. It, then, methods the statistics and applies a manipulate motion.

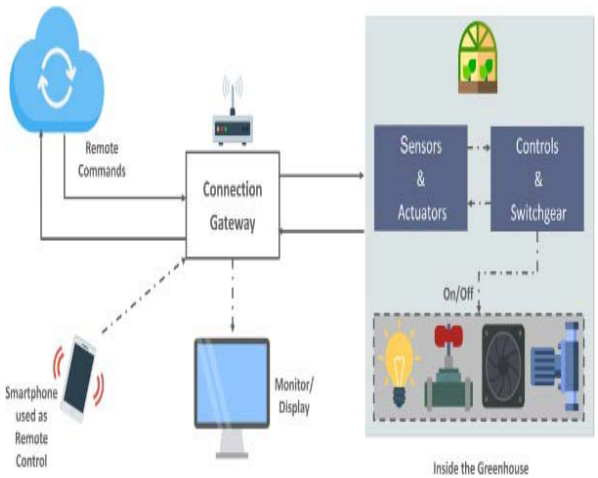


Figure 4: Greenhouse automation

c) Cattle monitoring and management

Just like crop monitoring, there are IoT agriculture sensors that can be connected to the animals on a farm to reveal their fitness and log overall performance. This works similarly to IoT gadgets for petcare. For example, SCR by Allflex and Cow la ruse smart agriculture sensors (collar tags) to supply temperature, health, hobby, and nutrition understandings on each person cow as well as collective records approximately the herd.

Figure 5: Cattle monitoring and management

V. Crop Management

One more kind of IoT product in agriculture and some other detail of precision farming are crop control gad gets. Just like climate stations, they should be located inside the field to collect records particular to crop farming; from temperature and precipitation to leaf water capability and typical crop fitness. Thus, you can display your crop growth and any anomalies to correctly prevent any diseases or infestations which could damage your yield. Arable and Semios can serve as precise representations of how this use case may be applied in actual life.

Figure 6: Cattle monitoring and management

VI. How IOT can Improve Agriculture

There are a few techniques of Internet of factors (IoT) for improve farming for agriculturalists. Agriculturalists can become concentrated sanctions from those policies.

1. Data, tons of statistics, amassed by means of smart agriculture sensors, e.g. Weather conditions, soil excellent, crop's growth progress or livestock's health. This records may be used to music the country of your business in smart as well as workers overall performance, tools effectiveness, and soon.
2. Improved switch over the internal methods and, as an end result, lower manufacturing dangers. The capability to foresee the output of your production lets in you to plot for advanced produce delivery. If exactly how much undergrowth you will crop, you could make convinced your produce increased lie about unsold.
3. Augmented commercial effectiveness through procedure mechanization. By using smooth strategies, you can mechanize numerous developments crossways your construction cycle, e.g. irrigation, composting, or pest control.
4. Budget organization and unused decrease recognitions to the augmented controller over the manufacture. Existence intelligent to see any irregularities in the harvest development or steers fitness, you will be able to moderate the hazards of behind your produce.
5. Improved creation superiority and capacities. Accomplish improved regulator finished the construction development and continue developed principles of produce excellence and growing volume finished mechanization.

VII. Challenges of IOT for Agriculture

a) The brain

Data analytics need to be at the central of every smart agriculture answer. The amassed information itself might be have little assist if you can't make sense of it. Thus, you want to have effective facts analytics capabilities and practice predictive algorithms and device studying in order to reap actionable insights based on the collective data.

b) The hardware

To create an Internet of Things answer for agriculture, you need to pick the sensors on your tool (or create a custom one). Your desire will depend on the kinds of particulars you want to obtain and the reason of your solution in preferred. In any case, the wonderful of your sensors is significant to the achievement of your product: it's going to depend on the accuracy of the collected data and its consistency.

c) The maintenance

Maintenance of your hardware is a project that is of number one importance for Internet of Things products in agriculture, because the sensors are usually used in the subject and may be effortlessly broken. Thus, you need to make sure your hardware is durable and clean to keep. Then you'll want to update your sensors more often than you would similar.

d) The mobility

Smart farming applications need to be tailored to be used within the field. A business owner or farm manager must be capable of get right of entry to the facts on website online or remotely through a telephone or desktop laptop. Plus, every linked tool must be self-sufficient and feature enough wireless diversity to connect with the opposed devices and transport truths to the important server.

e) The infrastructure

To make sure that your clever farming application performs well (and to make certain it may deal with the records load), you want a hard internal infrastructure. Furthermore, your internal structures ought to be cozy. Failing to correctly at easey our system only increases the likeliness of someone breaking into it, stealing your facts or even taking operate of your self-satisfactory tractors.

VIII. IOT Careers Opportunity

These are the following Career prospects in the Internet of Things:

a) Network and Structure

Internet of Things (IoT) device can be seemed as a complicated mesh of linked devices and devices that ultimately makes no feel if it isn't usually measured properly in advance than implementation. Because of the giant type of employments being completed and might be possible within the future, there are distinct varieties of sensors and transmitters that talk in a different way in the system. This is where the community specialization could are to be had in. There may be a big array of techniques of communicating statistics. Networking experts have been dealing with pc networks so far, and compared to IoT networks, that's a chunk of cake.

b) Data analytics

One of the key functions of an IoT gadget is the quantity of facts generated. With the sheer variety of devices concerned and now not something to make an experience of it, it's as top as a pile of junk. Records analytics are in excessive name for in the IoT organization with know- how in each dependent and unstructured facts. The based records come into play from specialized sensors that not only ship values. However, additionally the identifiers for the shape of

facts. Large information know-how and enjoy may be a sturdy factor in getting opportunities in this phase.

c) Protection

This is the current-day buzz word inside IoT. Unexpected explosion of device and sensor implementation, the industry has most effective now observed out that all that data and all the ones gadgets additionally need to be protected from malicious out of doors assets. If the security implementation to your smart refrigerator is inclined, and its miles linked to the identical network as your laptop, it might be pretty feasible, and in reality, easy for a hacker to apply this course on your personal data.

d) Device and Hardware

Hardware engineers are the folks who honestly prepare the diverse additives to be had to manufacture the tool in terms of a format. The equivalent is applicable to IoT as nicely, although with an enormous range of sensors and transmitters additionally, engineers and device authorities who can enforceable wireless, Bluetooth and other connectivity answers are also considerably favorite.

e) Cell and UI development

The IoT growth has come at a time wherein our lives are intently enclosed with smartphones. And because the complete factor of IoT is to connect everything all-the- time, smartphones and cellular devices are quality applicants for the platform of desire to manipulate IoT devices. Useless to say, this shows there is an excessive demand for android and ios builders in IoT. No longer that the ones roles without a doubt wanted any extra call for, however gift-day developers will want to gain an knowledge in running with programming libraries that permit apps to speak with outside devices and sensors.

IX. Smart Farming Tools

Smart Farming is a cultivated management perception using current device to development the amount and excellence of sophisticated properties. Agriculturalists in the 21st period have access to GPS, soil browsing, data management, and Internet of Things machineries. By confidently calculating differences within a field and familiarizing the approach consequently, Farmers can substantially increase the effectiveness of pesticides and stimulants, and use them greater selectively. Smart farming is call for of these days virtual global. Smart farming offer many capabilities like water nice, Plant health. Smart farming is a management idea targeted on offering the farming manufacturing with the arrangement to control advanced expertise which include huge information, the cloud and the internet of things (IoT) for following, looking, mechanizing and comparing approaches.

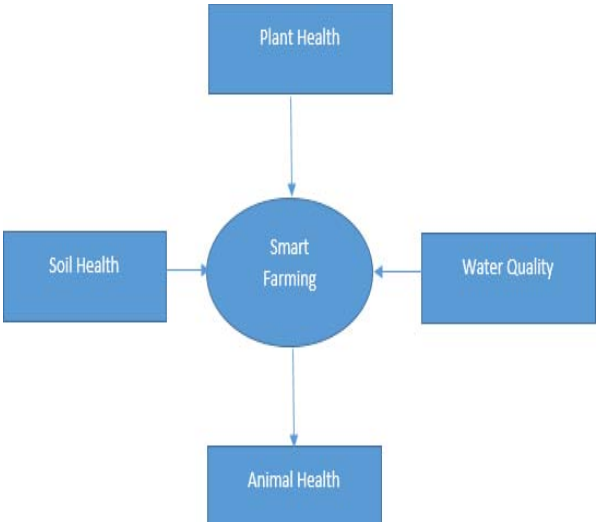


Figure 7: Smart farming

There are approximately smooth agricultural apparatuses are used by agriculturalists are:

Table 2: Tools of Smart farming

S. No.	Tools Name	Descriptions
1	Sensors	For soil scanning and liquid, light, humidity and high temperature management.
2	Telecommunications technologies	Advanced networking and GPS.
3	Hardware and software	For particular applications and for allowing IoT-based solutions, automation and mechanization.
4	Data analytics tools	Tools for decision making and prediction. Data collection is a significant part of smart farming as the quantity of data available from crop yields, soil- mapping, climate change, fertilizer applications, weather data, machinery and animal health continues to escalate.
5	Satellites and drones	For gathering data around the clock for an entire field. This information is forwarded to IT systems for tracking and analysis to give an “eye in the field” or “eye in the barn” that makes remote monitoring possible.

X. Conclusion

Internet of Things enabled agriculture has helped put into effect current technological answers to time examined understanding. This has enabled association the distance among manufacturing and nice and amount produce. Statistics Consumed by obtaining and introducing measureable from the more than one

instruments for real time use or garage in a database ensures fast action and much less harm to the vegetation. With seamless stop to quit wise operations and improved enterprise process execution, produce becomes handled faster and influences superstores in wildest time feasible. IoT farming solicitations are production it potential for farmers and agriculturalists to collect expressive statistics. Big property-owners and minor agriculturalists necessity appreciate the possible of IoT marketplace for farming by connecting smart know-hows to intensification attractiveness and sustainability in their manufactures. In this paper we study the Internet of Things (IoT) application for agriculture and how farmer can grow by using Internet of Things for agriculture. This paper study the careers opportunity of Internet of Things (IoT).

Ethics

This Research paper is original and not published in any conferences or in any journal.

References Références Referencias

1. R. Vignesh and 2A. Samydurai ans1 Student, 2Associate Professor Security on Internet of Things (IOT) with Challenges and Counter measures in 2017IJEDR|Volume5, Issue 1 | ISSN: 2321-9939.
2. N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, 203-209, 1987.
3. J. Y. Lee, W. C. Lin, and Y. H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1-2, 2014.
4. Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.
5. B. Anggorojati, P. N. Mahalle, N. R.Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network,"in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604-608,2012.
6. M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5,86-97,2012.
7. R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172,2014.
8. Mirza Abdur Razzaq and Muhammad Ali Qureshi "Security Issues in the Internet of Things (IoT): A Comprehensive Study" by (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 8, No. 6, 2017.
9. J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.
10. M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp.1–8.
11. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," IEEE Internet of Things journal, vol. 1, no. 4, pp. 349– 359, 2014.
12. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw. vol. 54, no. 15, pp. 2787–2805, Oct2010.
13. M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp.21–28.
14. L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233– 2243, 2014.
15. L.M.R. Tarouco, L.M. Bertholdo, L.Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J.J.C. de Santanna, "Internet of things in healthcare: Interoperability and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.
16. Mohan, "Cyber security for personal medical devices internet of things," in Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on. IEEE, 2014, pp. 372–374.
17. Mohamed Abomhara and Geir M. Køien" Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks".
18. S. De, P. Barnaghi, M. Bauer, and S. Meissner, "Service modelling for the internet of things," in Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on. IEEE, 2011, pp. 949–955.
19. G. Xiao, J. Guo, L. Xu, and Z. Gong, "User interoperability with heterogeneous iot devices through transformation," 2014.
20. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions, "Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
21. M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's intranet of things to a future internet of things: a wireless-and mobility-related view,"

Wireless Communications, IEEE, vol. 17, no. 6, pp. 44–51, 2010.
22. C. Hongsong, F. Zhongchuan, and Z. Dongyan, "Security and trust research in m2m system," in Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on. IEEE, 2011, pp. 286–290.
23. Cha, Y. Shah, A. U. Schmidt, A. Leicher, and M.V. Meyerstein, "Trust in m2 communication," Vehicular Technology Magazine, IEEE, vol. 4,no. 3, pp. 69–75, 2009.
24. Lopez, R. Roman, and C. Alcaraz, "Analysis of security threats, requirements, technologies and standards in wireless sensor networks."

Global Journals Guidelines Handbook 2020

www.GlobalJournals.org

Memberships

Fellows/Associates of Computer Science Research Council

FCSRC/ACSRC Memberships

Introduction

FCSRC/ACSRC is the most prestigious membership of Global Journals accredited by Open Association of Research Society, U.S.A (OARS). The credentials of Fellow and Associate designations signify that the researcher has gained the knowledge of the fundamental and high-level concepts, and is a subject matter expert, proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice. The credentials are designated only to the researchers, scientists, and professionals that have been selected by a rigorous process by our Editorial Board and Management Board.

Associates of FCSRC/ACSRC are scientists and researchers from around the world are working on projects/researches that have huge potentials. Members support Global Journals' mission to advance technology for humanity and the profession.

FCSRC

Fellow of Computer Science Research Council

FELLOW OF COMPUTER SCIENCE RESEARCH COUNCIL is the most prestigious membership of Global Journals. It is an award and membership granted to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Fellows are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Fellow Members.

Benefit

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A FCSRC member gets access to a closed network of Tier 1 researchers and scientists with direct communication channel through our website. Fellows can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Fellows receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Fellows can use the honored title of membership. The “FCSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., FCSRC or William Walldroff, M.S., FCSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Fellow members of FCSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation. All fellows get a dedicated page on the website with their biography.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Fellows receive discounts on future publications with Global Journals up to 60%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Fellows get secure and fast GJ work emails with unlimited forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, fellows receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Fellows are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All fellows receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 60% of sales proceeds

Fellows can publish articles (limited) without any fees. Also, they can earn up to 70% of sales proceeds from the sale of reference/review books/literature/publishing of research paper. The FCSRC member can decide its price and we can help in making the right decision.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Fellow members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

Access to Editorial Board

Become a member of the Editorial Board

Fellows may join as a member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. Additionally, Fellows get a chance to nominate other members for Editorial Board.

Career | Credibility | Exclusive | Reputation

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 5 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 10 GB free secure cloud access for storing research files.

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL

ASSOCIATE OF COMPUTER SCIENCE RESEARCH COUNCIL is the membership of Global Journals awarded to individuals that the Open Association of Research Society judges to have made a 'substantial contribution to the improvement of computer science, technology, and electronics engineering.

The primary objective is to recognize the leaders in research and scientific fields of the current era with a global perspective and to create a channel between them and other researchers for better exposure and knowledge sharing. Members are most eminent scientists, engineers, and technologists from all across the world. Associate membership can later be promoted to Fellow Membership. Associates are elected for life through a peer review process on the basis of excellence in the respective domain. There is no limit on the number of new nominations made in any year. Each year, the Open Association of Research Society elect up to 12 new Associate Members.

To the institution

Get letter of appreciation

Global Journals sends a letter of appreciation of author to the Dean or CEO of the University or Company of which author is a part, signed by editor in chief or chief author.

Exclusive Network

Get access to a closed network

A ACSRC member gets access to a closed network of Tier 2 researchers and scientists with direct communication channel through our website. Associates can reach out to other members or researchers directly.They should also be open to reaching out by other.

Career | Credibility | Exclusive | Reputation

Certificate

Certificate, LoR and Laser-Momento

Associates receive a printed copy of a certificate signed by our Chief Author that may be used for academic purposes and a personal recommendation letter to the dean of member's university.

Career | Credibility | Exclusive | Reputation

Designation

Get honored title of membership

Associates can use the honored title of membership. The “ACSRC” is an honored title which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., ACSRC or William Walldroff, M.S., ACSRC.

Career | Credibility | Exclusive | Reputation

Recognition on the Platform

Better visibility and citation

All the Associate members of ACSRC get a badge of "Leading Member of Global Journals" on the Research Community that distinguishes them from others. Additionally, the profile is also partially maintained by our team for better visibility and citation.

Career | Credibility | Reputation

Future Work

Get discounts on the future publications

Associates receive discounts on future publications with Global Journals up to 30%. Through our recommendation programs, members also receive discounts on publications made with OARS affiliated organizations.

Career | Financial

GJ Account

Unlimited forward of Emails

Associates get secure and fast GJ work emails with 5GB forward of emails that they may use them as their primary email. For example, john [AT] globaljournals [DOT] org.

Career | Credibility | Reputation

Premium Tools

Access to all the premium tools

To take future researches to the zenith, associates receive access to all the premium tools that Global Journals have to offer along with the partnership with some of the best marketing leading tools out there.

Financial

Conferences & Events

Organize seminar/conference

Associates are authorized to organize symposium/seminar/conference on behalf of Global Journal Incorporation (USA). They can also participate in the same organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent. Additionally, they get free research conferences (and others) alerts.

Career | Credibility | Financial

Early Invitations

Early invitations to all the symposiums, seminars, conferences

All associates receive the early invitations to all the symposiums, seminars, conferences and webinars hosted by Global Journals in their subject.

Exclusive

Publishing Articles & Books

Earn 30-40% of sales proceeds

Associates can publish articles (limited) without any fees. Also, they can earn up to 30-40% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.

Exclusive | Financial

Reviewers

Get a remuneration of 15% of author fees

Associate members are eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get a remuneration of 15% of author fees, taken from the author of a respective paper.

Financial

And Much More

Get access to scientific museums and observatories across the globe

All members get access to 2 selected scientific museums and observatories across the globe. All researches published with Global Journals will be kept under deep archival facilities across regions for future protections and disaster recovery. They get 5 GB free secure cloud access for storing research files.

Associate	Fellow	Research Group	Basic
$4800 **lifetime designation**	$6800 **lifetime designation**	$12500.00 **organizational**	APC **per article**
Certificate, LoR and Momento **2** discounted publishing/year **Gradation** of Research **10** research contacts/day **1 GB** Cloud Storage **GJ** Community Access	**Certificate,** LoR and Momento **Unlimited** discounted publishing/year **Gradation** of Research **Unlimited** research contacts/day **5 GB** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**Certificates,** LoRs and Momentos **Unlimited** free publishing/year **Gradation** of Research **Unlimited** research contacts/day **Unlimited** Cloud Storage **Online Presense** Assistance **GJ** Community Access	**GJ** Community Access

Preferred Author Guidelines

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

Before and during Submission

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, “What words would a source have to include to be truly valuable in a research paper?” Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10.Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350