Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

WSN BASED SENSING MODEL FOR SMART CROWD MOVEMENT WITH IDENTIFICATION: AN EXTENDED STUDY

[1,3]NAEEM A. NAWAZ, [2]AHMAD WAQAS, [3]ZULKEFLI MUHAMMED YUSOF, [4]ABDUL WAHEED MAHESAR, [5]ASADULLAH SHAH

[1]Department of Computer Science, International Islamic University Malaysia

[2]Department of Computer Science, Sukkur Institute of Business Administration, Pakistan

[3]Department of Computer Science, Ummul Qura University, Makkah, Kingdom of Saudi Arabia

E-mail: [1]nanawaz@uqu.edu.sa, [2]ahmad.waqas@iba-suk.edu.pk, [3]abdul.waheed@live.iium.edu.my, [4]zulmy@iium.edu.my, [5]asadullah@iium.edu.my

ABSTRACT

With the advancement of IT and increase in world population rate, Crowd Management (CM) has become a subject undergoing intense study among researchers. Technology provides fast and easily available means of transport and, up-to-date information access to the people that cause crowd at public places. This imposes a big challenge for crowd safety and security at public places such as airports, railway stations and check points. For example, crowd of pilgrims during Hajj and Ummrah while crossing the borders of Makkah, Kingdom of Saudi Arabia. To minimize the risk of such crowd safety and security, identification and verification of people is necessary which caused unwanted increment in processing time. It is observed that managing crowd during specific time period (Hajj and Ummrah) with identification and verification became challenge. At present, many advanced technologies such as Internet of Things (IoT) are being used to solve the crowed management problem with minimal processing time. In this paper, we have presented a Wireless Sensor Network (WSN) based conceptual model for smart crowd movement with optimal verification of cluster members (CMs) and leads to minimal processing time for people identification. This handles the crowd by forming groups and provides proactive support to handle them in organized manner. As a result, crowd can be managed to move safely from one place to another with group identification. By controlling the drop rate or unverified CMs rate, the performance of the smart movement can be increased. This decrease or control of the drop rate will also minimize the processing time and move the crowd in smart way.

Keywords: *WSN, Crowd Management, Smart Movement, IoT, CMs*

1. INTRODUCTION

Safety and security are most concerned issues at crowded areas which could be controlled and minimized if crowd move from one place to another place with identification. As a matter of fact, individual identification consumes processing time and effort that increases risk of crowd safety. The identification time of crowd may be minimized if the identification is automatically performed in form of groups. The efficient crowd processing is required, during the event of Hajj (an important pillar of Islam), more than 5 million pilgrims get together in Makkah, the holy city in Kingdom of Saudi Arabia, in order to perform Hajj [1]. In the same way, more than 14 million Muslims perform Ummrah in Makkah in a calendar year [2]. This crowd of pilgrims moves to different places such as hotels, Al-Haram, Mina, Arfaat, Mudaulfah and Jamraat. Also from different airports to the Holy cities of Makkah and Madinah. At present, data of pilgrims is recorded at airport and is verified at different check points such as boarders of Makkah, Minna and Arfaat. It is observed that individuals have to wait for long while their data is captured at different places such as airports, railway stations and check points at Makkah boarders etc. We have presented a Wireless Sensor Network (WSN) based smart crowd movement model that automatically identifies individuals in form of groups to address the problem of long waiting time. The proposed model consists of different operational phases and grouping technique to collect, disseminate and process crowd data for identification.

Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The concept of cloud computing is to provide the services to the large number of consumers globally via Internet in efficient way which are located on many different locations while the resources (Hardware and Software) are located on few physical locations [3][24][25].

By definition, Inter of Things (IoT) allows people/anybody and things/devices to be connected anytime, anyplace/anywhere, with anything and anyone, ideally using any path/network and any service [4]. It is one of the basic need of the peoples (Pilgrims or Hajjaj) and Hajj or Ummrah management to use IoT to get updated information to control and mange different factors. Information received by IoT can be used by the controlling/management body such as traffic police, police stations, ministry of interior, food supplying companies for different purpose for instance finding hotel or camp location in Mina and Arafat, traffic control, temperature, humidity, overcrowded area, food and other supplies. The identification of eight critical factors of smart city initiatives are management and organization, technology, governance, policy context, people and communities, economy, built infrastructure, and natural environment [5]. These factors form the basis of an integrative framework that can be used to examine how local governments are envisioning smart city initiatives. The framework suggests directions and agendas for smart city research and outlines practical implications for government professionals [6].

The clustering phenomenon plays an important role to manage and affect the performance of the WSNs. There are several key limitations in WSNs, the grouping schemes must consider. For Example, limited energy, network lifetime, limited abilities, and applications [7].

As during the Hajj and Ummrah, the city of Makkah is crowded and these are the days to manage the crowd in smart way. Smart way means crowd move from one place to another place with safety, security, identification and in short time. This goal can be achieved by processing the crowd in group form with the help of WSNs model and operational phases.

This paper is an extension of our previous work presented and published in the proceedings of IADIS International Conference on Web Based Communities 2016 [8].

1.1. Sensing-as-a-Service Model

The main idea of sensing as service model for smart cities with support of Internet of Things is to provide benefit to the data owner as well as to the data consumers [9]. For example, the data is sensed by sensors embedded inside the refrigerator. The sensor publisher collects data from the refrigerator and sells to the data consumers with the permission of data owner. The data consumer can access data by requesting to the data publisher or extended service provider and pay for it to data owner. The model is composed of four layers namely sensor and sensor owner, sensor publishers, extended service provider and data consumers as shown in Figure 1.

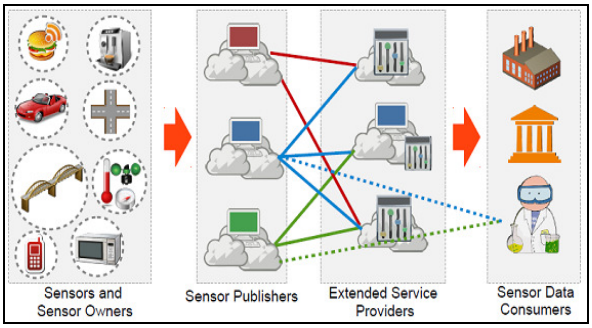

Figure 1: Sensing as a Service Model [9]

- Sensors and Sensor Owners Layer: This layer consists of sensors and sensor owners. A sensor is a device that detects, measures or senses a physical phenomenon such as humidity, temperature, etc. Sensors are embedded in variety of devices and are owned by sensor owners [10].
- Sensor Publishers Layer: This layer consists of sensor publishers (SP). The main responsibility of a sensor publisher is to detect available sensors, communicate with the sensor owners, and get permission to publish the sensors in the cloud. Sensor publishers are separate business entities. When a sensor owner registers a specific sensor, SP collects information about the sensor availability, owner preferences and restriction, and expected return, etc.
- Extended Service Providers Layer: This layer consists of extended service providers (ESP). This layer can be considered as the most intelligent among all the four layers which embed the intelligence to the entire service model. The services provided by ESPs can be varied widely from one provider to another. However, there are some fundamental characteristics of ESPs, they have to provide value added services such as location tracing, supply-demand and crowd counting [4] to the sensor data consumers.
- Sensor Data Consumers Layer: This layer consists of sensor data consumers. All the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

sensor data consumers need to register themselves and obtain a valid digital certificate from an authority in order to consume sensor data. Some of the major sensor data consumers would be governments, business organizations, academic institutions, and scientific research communities.

1.2. The Hajj Crowd and Challenges

During the event of Hajj (an important pillar of Islam), more than 5 million pilgrims get together in Makkah, the holy city in Kingdom of Saudi Arabia [1]. In the same way, more than 14 million Muslims perform Ummrah in Makkah in a calendar year [2]. This crowd of pilgrims moves to different places and areas to fulfill the requirements and stay there for different days. These participants are registered with their native Hajj organizers (native government mission or private Hajj tour operators) as well as Saudi government and their designated offices. Still, when such a massive bunch of people try to perform Hajj rituals in a bounded region within a defined time frame; the issues like safety, security, integrity, health, tracking, tracing of all the participants, becomes a matter of extreme concern for all the stakeholders (i.e. Saudi government, Saudi Hajj officials, native Hajj organizers, and individual participants etc.).

On one side, the organizers are struggling to conduct the event without accidents or critical incidents such as stampedes, fire or medical emergencies. While on the other side, the participants and their local/native organizers are struggling to keep their groups combined, avoid dispersing of their group during crowded set of rituals, finding the lost and missing ones from their group etc. Even individuals face cases such as getting lost; getting dispersed from groups or from friends and families; locating the peers; re-gathering with groups or friends and families; directions and shortest paths to the next land mark etc.

In short there are countless challenges (from multiple perspectives), possessed by such crowded events, which can be addressed by available state of the art technologies. In this research, we intent to study the use of the available technologies according to the nature of the problem. Our intent is to propose a solution which can help address the challenges faced in such crowded (mass gathering) events.

2. RELATED WORK

The concept of sensing as a service is explored and investigated by Perera et al [11]. The objective is to investigate the concept of sensing as a service model in technological, economical, and social perspectives and identify the major open challenges and issues. The billions of devices that can sense, communicate, compute and potentially actuate are investigated by Arkady et al [12]. Data streams coming from these devices will challenge the traditional approaches to data management and contribute to the emerging paradigm of big data. A Centralized Dynamic Clustering approach in WSNs proposed by Fuad et al [13]. In CDC approach, adaptive clustering protocol organizes where the cluster head is responsible. For example, collecting the data from all the cluster members, aggregating the data, transmitting fused information to the base station and selecting new cluster head for next round. A distributed data collection algorithm proposed by Aly et al [14] for the storage problem. The clustering storage algorithm runs in different phases. Assume that the sensor network has 80% sensing nodes, and 20% storage nodes. All clusters in the network are established using clustering algorithms [15], [16]. A networked Distributed Storage Algorithm for WSNs and study its encoding and decoding operations presented by Aly et al [17]. Other previous algorithms assume that k source nodes disseminate their sensed data throughout a network with n storage nodes using the means of Fountain codes and random walks. However, in this work they generalize this scenario where a set of n sources disseminate their data to a set of n storage nodes. Also, in this proposed algorithm they used properties of WSNs such as broadcasting and flooding.

The term Internet of Things was first coined by Kevin Ashton in 1999 in the context of supply chain management [18]. However, in the past decade, the definition has been more inclusive covering wide range of applications like healthcare, utilities, transport, etc. [19]. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Radio Frequency Identification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities [20]. The next generation of WSN will benefit when sensor data is added to blog, virtual communities, and social network

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

applications. This transformation of data derived from sensor networks into a valuable resource for information hungry applications will benefit from techniques being developed for the emerging Cloud Computing technologies. Traditional High Performance Computing approaches may be replaced or find a place in data manipulation prior to the data being moved into the Cloud [26][27]. A novel framework is proposed to integrate the Cloud Computing model with WSN. Deployed WSN will be connected to the proposed infrastructure. Users request will be served via three service layers (IaaS, PaaS, SaaS) either from the archive which is made by collecting data periodically from WSN to Data Centers (DC), or by generating live query to corresponding sensor network [28]. Overcrowding that happens in places like concerts, stadiums or pilgrimage locations might sometimes cause injury or loss of life. Maintaining the safety of crowd in these places is therefore very important. In addition, increasing the performance of the buildings and structures has always been an important concern. Most of the previous work focused on using new devices and methods for monitoring and management of the crowd but they rarely focus on a comprehensive and structured approach with the purpose of increasing efficiency and safety.

Due to one by one individual processing, the existing system is unable to process the crowd speedily or it goes for random identification and verification. Furthermore, if crowd processing is done in cluster form and data is pre-written on the devices, then crowd processing time can be reduced. By using cluster crowd processing, we do not need the random identification and verification because cluster processing minimizes the time.

3. THE PRESENT IMPLEMENTATION OF CROWD PROCESSING

The present implementation of hajj crowd processing is done individually one by one and different steps are involved to process the hajj crowd at airport. The crowd processing for identification and verification is time taken and tiresome. But in case of check points (Makkah boarder) the identification is done randomly, which is again tiresome job and increases the security risk. The random identification is done because it takes a lot of time to process hajj crowd individually one by one. In case of the huge crowd (at Mina and Arfaat) there is no such check and balance for crowd identification. Although on railway stations at jamraat, Mina, Muzdulfah and Arfaat there are scanners for tag verification. But this verification is done one by one and it is difficult to perform verification in this way at times of huge crowds. To overcome the problem of crowd processing, WSN based sensing model is proposed which supports crowd processing in cluster form and has the cluster members, cluster head and servers with prewritten data.

4. PROPOSED MODEL FOR SMART MOVEMENT

A WSN based smart crowd movement model along with its operational phases is illustrated in Figure 2. The figure provides the understanding and flow of the data, and functions of each components in the proposed model. Moreover, it illustrates the flow of each phase that is involved to collect, store, disseminate and identify the crowd in smart way. The sensor device is not only a data collector and data transmitter; it can be used for multiple purposes such as:

i. Forming the groups of sensor devices and group of sensor devices manage by the master or group device (cluster head).
ii. Identification of the group members
iii. Verify the data in the form of groups

The main idea of the model in Figure 2 is taken from the sensing as a service model for smart cities. In the existing model four layered architecture is used that are sensor and sensor owner, sensor publishers, extended service provide and data consumers. The data is sensed by sensors with the permission of owner and stored by the sensor publishers. The data consumer can access data by requesting to the data publisher or extended service provider. The proposed model in Figure 2 is different than the previous model and work by clustering or grouping sensors and different operational phases.

In Figure 2, proposed wireless sensor network and clustering or grouping model has different components as given:

- **Cluster or groups:** The dense nature of crowd requires to be organized into clusters or groups in order to simplify tasks such a processing [23].
- **Cluster or group heads:** Cluster or group head is the organizer or leader of a cluster or group [23]. They often are required to organize activities in the cluster or group.
- **Base Station:** The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

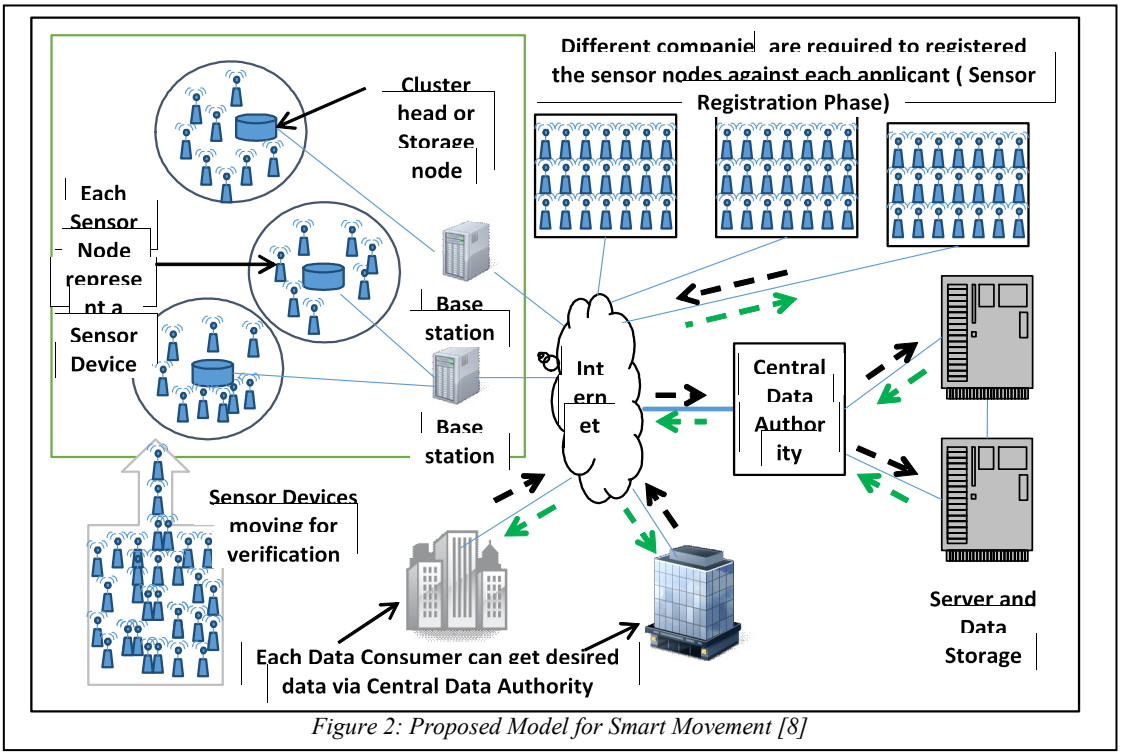

Figure 2: Proposed Model for Smart Movement [8]

- **End User:** The data in a sensor network can be used for a wide-range of applications. Therefore, a particular application may make use of the network data over the Internet, using a mobile, PDA, iPad or even a desktop computer.
- **Sensors and Sensor Owners Company:** This includes the sensors devices (sensor nodes, smart device) and sensor owners' companies responsible for the specific group of peoples. A sensor is a device which read the information about humidity, number of peoples, number of vehicles, temperature, and wind speed by measuring or sensing [16].
- **Central Data Authority:** Central Data Authority will play a vital role for privacy and security of the data. The people, the companies, government, business organizations, institute or research authorities can access the data if they are registered member of Central Data Authority. This authority also checks which kind of data is accessible by the different members. This authority may offer the different package about data access.
- **Sensor Data Consumers:** All the sensor data consumers need to get registered and obtain a valid digital certificate from a central data authority in order to access sensor data. Some of the major sensor data consumers are Traffic Control, Ministry of interior affairs, Police stations, Traffic wardens, hospitals, business organizations, academic institutions, and scientific research communities. Data consumers can access the data according to the privileged packages.

At present, most of the available wireless sensor devices have considerable limitations in terms of computational power, memory, efficiency and communication capabilities due to economic and technology reasons. The development of low-cost, low-power, a multifunctional sensor has gained attention from various industries for different applications. One such research problem is to create an organizational structure amongst these nodes [10].

By clustering or grouping the sensor nodes the processing power can be increased which subsequently decrease the time for processing high density data at public or overcrowded areas such as airports, railway stations, check points especially during Hajj and Ummrah, crossing of Makkah boarders etc.

The combination of the WSN with telecommunication, Internet and other network devices will play vital role to collect, disseminate and process high density data globally. By the deployment of billions of sensor devices big amount of data can be sensed, stored and required to process and to get results for different applications [9].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.1. Operational Phases

To manage the crowd in smart way, the proposed WSN model considers the operational phases (can be further sub divided) given as:

- Sensor Registration Phase: In this phase, sensors need to be registered. As an example of Hajj and Ummrah, as the application is approved, each company will provide approved applicant documents to the Central Data Authority. The Central Data Authority will verify the documents and register the applicant on web and also register a sensor device against each applicant. Each registered sensor device will have applicant personal information, visa number, passport number, their specific route, booking of rooms, Camp (Tent) in Mina or in Arfaat according to day and date.
- Sensor Dispatching Phase: In this phase, the registered sensor devices are handed over to the company that has submitted the documents for registration of the applicants. There are different options to dispatch registered sensor devices to the applicants.
  i. Dispatching registered sensor devices to the ministry of concern country and the applicants get their devices from ministry after verification.
  ii. Each company dispatch registered sensor devices to their sub offices in each country and applicants get the registered sensor device from sub offices after verification.
  iii. Applicants verified by company at airport and provide registered sensor device to the concern applicant.
- Sensor clustering or grouping Phase: In the dispatching phase, the registered sensor device is given to applicants after verification. The data for a cluster or group of registered devices will stored in a main device that is called the cluster or group head. The cluster or group devices data will be matched by the cluster or group head device. If the data is matched, then cluster or group members will present in front of immigration in a specific zone or area.
- Cluster or group Sensing Phase: In the sensing phase, the Group or cluster head device will be sensed by the immigration system for data collection instead of individual sensing of each device.
- Cluster or group Verification Phase: As all the sensor devices are registered and data is stored on servers, the sensed data will be verified and the applicant's status will be updated by the name of entry point (Airport name). For each verification point, applicant's status will be updated by the name of entry point. For Example, Jeddah airport, Makkah boarder, Minna and Arfaat etc. This update of the entry point will define the route followed by the user carrying the sensor device. For organized movement, a specific route for different groups can be defined according to date and time so that one path does not get overcrowd.

4.2. Use-case for Smart Crowd Movement

The Company inviting the people for Hajj, Ummrah or visit is responsible to complete the process of visa or permit. As the process of visa completed, the company will define information about route of their travel and booking plan at different locations (City, Hotel). Company will register the sensor device for individuals to Central Data Authority. The company will provide the documents having personal information of the people coming for Hajj, Ummrah or visit under their supervision to the authority.

In the first phase sensors are registered for the specific applicant by the company. These sensing devices can be provided to the people at their arrival at airport, in ministry of their country or sub office of the company in their country after manual verification. The data will be collected by the cluster or group head and verified at once by the immigration system in the form of cluster or group. When the people are managed to get into the bus (vehicles) the passenger verification will be performed automatically before entering into the bus and seat number will be allocated according to memory location in cluster or group head device. Passengers can be verified by the vehicle responsible authority or company. Bus status can be automatically verified at checkpoint.

When bus reaches to the checkpoint, the data will automatically be collected from the cluster or group head device via access point. If all passengers are verified successfully (All number of passengers stored on cluster or group head device verified by server), then there is no need to step into the bus and verify the passengers manually. If there is some problem with verification of any passenger (device failure) the cluster or group head device will mention the seat number (memory location) so that verification for that specific passenger can be performed. Communication between cluster or group head device and checkpoint terminal can be done via WiFi, Bluetooth or 4G link. In worst wireless connection scenario, cluster or group head device has the capability to connect via wired connection as backup option to verify the data. At

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

each checkpoint, whole bus passengers will be verified by using the data stored by the cluster or group head. When bus enters into the city the route of hotel for concern group will be mentioned by the cluster or group head device.

4.3. Preliminary Analysis

The existing system crowd processing is explained in the section 3 that includes manual and computerized systems. The proposed system explained in the section 4. Here we discussed the preliminary analysis and comparison between existing crowd processing and proposed smart crowd processing as given in Table 1.

Table 1: Preliminary Analysis between Proposed and Existing Model

Proposed Model	Existing Model
Smart sensor device is used	Individual RFID tags are used partially
Data is collected in cluster or group form	Data is collected individually
Data access verification is done by the central data authority (Government)	No proper data access verification
Data verification is done at multiple points (at each checkpoint)	Data verification is done randomly and at some check points (Railway station)
Pre-registration for sensor device and data with identification	Post-registration for RFID and data
Cluster head devices are moving	RFID Gates are static
Every time central data authority gives access of data to the cluster head	No concept of cluster head data access.
Cluster or group approach	Individual or one by one approach

In the preliminary analysis, we discuss the different aspect of both of existing and proposed models. In the existing model, individual RFID tags are embedded at some points to count the number of pilgrims without identification but in our conceptual WSN sensing model a smart device is used which can perform different functions such as; sending, receiving and verification of the data etc. In the existing model, data is collected from individual RFID tags but in proposed model the data is collected in group or in cluster form by cluster head. In existing model, there is no proper data access verification, only responsible authority access the data and provide to other authorities at later stage. But in case of proposed model, the data access verification is done by the central data authority (Government). The data access is provided by the central data authority according to the data consumer needs. Data verification is done randomly at some check point such as railway station in case of the existing model but in case of the proposed model the data verification is done at multiple times at different check points. In existing model, RFID tags registration is done without recording the personal information but in case of the proposed model, sensor device is pre-registered at the time of completion of the visa process with prerecorded personal information. In existing model, the RFID gates are fixed without concept of the cluster head but in case of the proposed model the cluster head devices are moving because they are carried by the persons. In existing model, once the responsible authority gives the access of the data, data consumers are free to access the data. But in case of proposed model each time central data authority provides access of data to the cluster head and list of the CMs updated by the central data authority. In the existing model data carried by the sensors are not sensitive, it provides the valid RFID tag number but in case of the proposed model, the sensor device has personal information such as; Name, visa number, passport etc. that is a sensitive and important information. In the existing model, individual or one by one approach is used to process the crowd and provide data to the data consumers at later stage. In case of proposed model, cluster or group approach is used to process the crowd that includes registration, dispatching, clustering, sensing and verification phases.

5. CLUSTER (GROUP) ALGORITHM

In cluster algorithm, we discuss the algorithm that represents the scenario of cluster and its members. We discussed the number of verified and unverified cluster members by increasing the number of the cluster members in a cluster. All cluster members remain within the cluster head transmission range. Different cluster situations (scenarios) represented are: all cluster members belonging to the same and within transmission range of cluster head; all cluster members belonging to the same cluster head but some are out of the transmission range of cluster head; cluster members belonging to a different cluster head but within transmission range of their own cluster head; and cluster members belonging to different cluster head but some are out of the transmission range of their own cluster head. According to the different

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

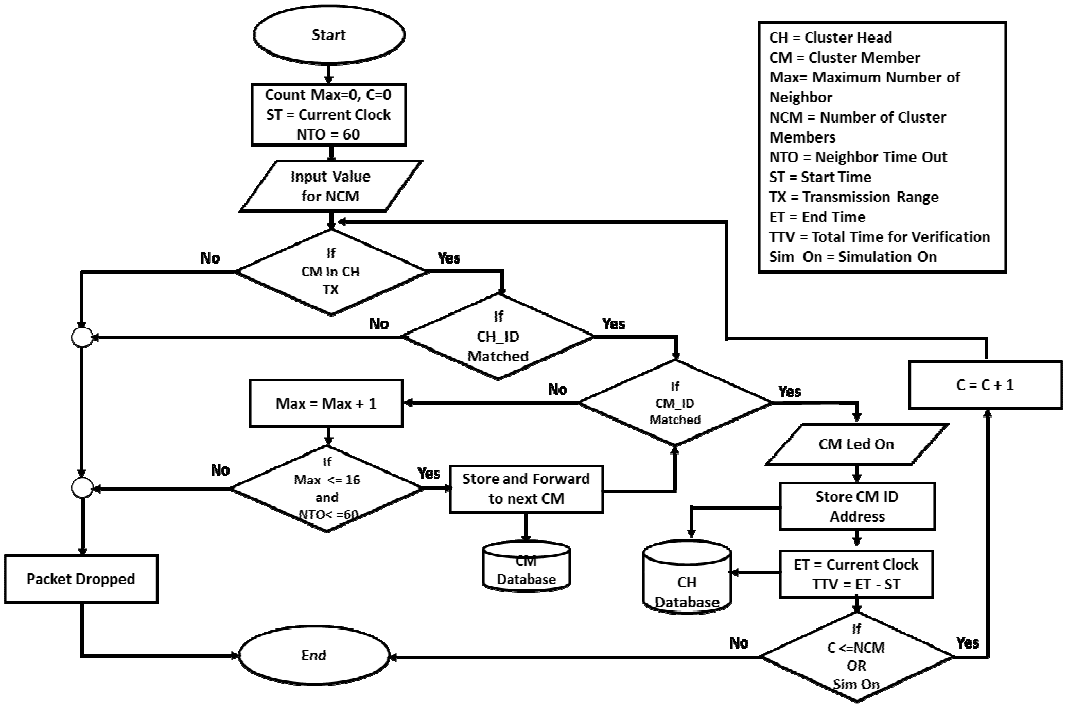

Figure 3: Flowchart for Different Number of Cluster Members Verification

given algorithms, we write codes for different situations (scenarios) of cluster.

In Figure 3, the flowchart represents the number of cluster members supported by the proposed system. We first put 5-number of cluster members and check the number of cluster members verified. We increase the number of cluster members by multiples of 5 to check the maximum number of the cluster numbers supported by the cluster head. The simulation and results of the given algorithm are given in the next session. In flowchart, at the start, some of the variables are initialized and synchronize with the environment. Initialization allocate values to Neighbor Time Out (NTO) in second, Max is counter for maximum number of neighbor and C as counter. The algorithm facilitates the user to enter the number of cluster members. Verification of the CM is done on the basis of CH_ID and CM_ID. CH_ID represents the uniqueness of the cluster head and CM_ID represent the uniqueness of the CM in the cluster. After verification of the CH_ID and CM_ID, the CM led turns on (Green) as a proof of verification. Green light will make separation between verified and unverified CM easier. After each counter, the memory of CH updates and stores the values for CM_ID, ET and TTV. Where ET represents the Ending Time of verification and TTV represents Total Time for Verification. If CM_ID does not belong to the current CH, the counter Max will be increased by one and a packet will be forwarded to the next neighbor (next CM). The information of where the packet is going to be forwarded is stored in the neighbor table of CM. Before forwarding a packet to next CM, it checks the NTO and Max values. If value does not exceed to its maximum values then, it stores the information in CM memory and compares the CM_ID of the received packet and the current CM_ID. Then CM_ID is verified. But if NTO or Max value exceeds the maximum limit, then packet will be dropped. This algorithm remains executing until maximum number of CMs (NCM) are reached or simulation time is over.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithm 1: Algorithm for Different Number of Cluster Members Verification

```
Step-1  Begin
Step-2  Set Max=0, C=0
Step-3  Set NTO=60 sec, ST=Current (clock)
Step-4  GET value for NCM
Step-5  If (CM in TX of CH)
Step-6          If(CH_ID == Current (CH_ID))
Step-7                  If(CM_ID == Current (CM_ID))
Step-8                          Display CM LED ON(GREEN)
Step-9                          CH(Database) ← (CM_ID,ET, TTV)
Step-10                                 If(Sim ON || C <= NCM)
Step-11                                         C=C+1
Step-12                                         GOTO Step-5
Step-13                                 Else
Step-14                                         GOTO Step-29
Step-15                 Else
Step-16                         Max=Max+1
Step-17                                 if(Max<=16 && NTO<=60)
Step-18                                         GOTO  → Next(CM)
Step-19                                         CM(Database) ← (CM_ID)
Step-20                                         GOTO Step-7
Step-21                                 Else
Step-22                                         Remove(Packet)
Step-23                                         GOTO Step-29
Step-24                 Endif
Step-25         Else
Step-26                 Remove (Packet)
Step-27         Endif
Step-28 Else
Step-29         Remove (Packet)
Step-29 Endif
```

6. SIMULATION ENVIRNMENT

The algorithms are implemented on WSN based scenarios that are developed to validate the proposed simulation model. At first, the results for different number of CMs a cluster (Group) are presented. The results for verified and unverified CMs in a cluster are explained by controlling and varying the number of CMs in cluster. The results for proposed system are calculated and estimated in terms of total number of of cluster members verified and verified. The results show in Table 2, and by graph in Figures 5(a) and 5(b). After that, the drop rate (unverified Nodes) increases which increases the crowd processing time. The optimal number of CMs are 20, where all of the CMs are verified and (unverified) drop rate is zero. The verified and unverified rate shows that WSN based framework can verified CMs in cluster form that leads to minimize crowd processing time. The simulation environment with parameters is given in the Table 2.

Table 2: Simulation parameters

Simulation Parameters	Values
Number of Cluster Members	5, 10, 15, 20, 25, 30, 35, 40, 45, 50
Transmission Range	50 m X 100 m
Startup Delay	1000 ms (1 sec)
Neighbor Timeout	60 sec
Max Neighbor	16
Position	Random
Simulation Time	5 min
Communication	Multi hop
Radio Channel	26
Protocol	CSMA MAC Contiki

To study the validity of proposed framework, Cooja/Contiki Simulator is used. In Table 2, the simulations parameters are mentioned for simulating the proposed WSN based sensing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

framework to calculate the number of verified, unverified and processing time for crowd in cluster form.

- **Number of Cluster Members:** The number of cluster members existing (populated) in a single cluster
- **Transmission Range:** The coverage area of the cluster head
- **Startup Delay:** Simulation startup delay to get ready for communication
- **Neighbor Timeout:** The time at which the old neighbor entry will be removed so that the table doesn't over flow.
- **Max Neighbor:** The maximum number of neighbors that can be supported. As the number of neighbors are increased, the number entry in the table will increase. It will require more memory and causes more delay.
- **Position:** The x and y coordinate of the CM's position. It can be defined as linear, elliptical, random or manually.
- **Simulation Time:** The time at which the simulation is completed to get required results.
- **Communication:** The multi-hop communication will help to forward the packet to the next neighbor if the destination CM is at a longer distance and in this way save the energy of CM. It will also help deliver the packet if the node is out of the cluster head's range.
- **Radio Channel:** Cooja/contiki support different radio channels for communication.
- **Protocol:** CSMA MAC is a Contiki lightweight protocol designed for low power, low memory and low processing power wireless sensor network.

7. SIMULATION RESULTS AND PERFORMANCE

7.1. Network Analysis Metrics to Identify (Verify) Cluster Members

There are different performance metrics to evaluate crowd processing in cluster form. Most of them include number of verified and unverified CMs in a cluster.

7.2. Verification by Existing System

Currently verification is done in queue form one by one or person by person. There are different steps are involved for the process of verification. This queue form verification cause a long queue and delay.

7.3. Number of Verified and Unverified Cluster Members

To validate our WSN based sensing model results, we evaluated the crowd in cluster form to find out the number of CMs supported by each cluster head. We randomly populated the member nodes as in our proposed system people exist randomly. The member nodes have pre-written information of people and cluster has pre-written list of the cluster members. Each cluster head is identified by the cluster head ID (CH_ID) and each cluster member is identified by CH_ID and CM_ID (Visa Number in this case). We gradually increased the number of cluster members by multiples of 5 (5, 10, 15 . . . 50). Our WSN based framework run smoothly and provided the number of verified and unverified cluster members. Simulation results are shown in Table 2. The number of unverified CMs are zero up to 20 number of CMs in a cluster. But at 25 number of CMs, number of verified CMs are 22 and the unverified CMs are 3 (3 out of 25 CMs). As the number of CMs increased, the number of unverified CMs also increased but number of verified CMs decreased gradually as shown in Figure 5 (a) and (b). Increasing the number of member nodes increases the number of neighbour's entries in the neighbour table (The table in which each CM keeps record of its neighbour). When it exceeds the maximum number of entries in a neighbour table, it causes dropping or removing of the entries from neighbour table. The dropping of entries causes the incomplete route to destination therefore packet drops. The second reason is that it exceeds the maximum number of neighbours and therefore drops the packet. In our case the maximum number of the neighbour limit is 16. The third reason is that WSN based frameworks work on the MAC layer and it uses the CSMA contiki protocol. CSMA does not support collision detection but when collusion happens it retransmits the packets after a certain time period. It causes delay in packet delivery and hence unverified or drop rate increase. As we increase the number of CMs, it increases the traffic that increases the chances of more number of collisions and hence packet drops before reaching the destination. In Figure 5(a) column chart and Figure 5(b) line chart, it can be seen that the number of the unverified CMs are zero when the number of CMs in the cluster are 20. As we increase the number of the CMs 25 the number of unverified CMs become 3. It can be seen that the number of verified CMs (17) remains more than the number of unverified CMs (13), when the number of the CMs increased up to 30 in cluster. The number of verified CMs start

Journal of Theoretical and Applied Information Technology
15th March 2017. Vol.95. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

decreasing (14) as compared to unverified CMs (21), when the number of cluster members increased up to 35 CMs. The trend showed that by increasing the number of the CMs in cluster, unverified CMs increased gradually but the decrease in number of verified CMs is up and down with small difference. From the Table 2 it can be seen that maximum number of verified CMs are 22 out of 25 and maximum number of dropped CMs are 36 out of 50. This means the optimal number of the CMs in a cluster is 20 because all CMs are verified and there are no unverified CMs. But as we increase the CMs in cluster 25 or more than 25 the number of unverified CMs increase gradually. We also try to increase the number of CMs more than 50 but simulation tool hangs up.

In Figure 4(a), all of 20 CMs are verified and there is no unverified CM. Here the cluster head ID is represented by 1 and from 2 to 21 are the IDs for CMs. The green LED represents the verified CMs.

Figure 4(a): All of 20- CMs are verified by the cluster head

In Figure 4(b), 22 CMs are verified and 3 CMs are unverified. Here the cluster head ID is represented by 1 and from 2 to 26 are the IDs for CMs. The green on LED represent the verified CMs. CMs with IDs 20, 21 and 26 are unverified because their green LED is off.

In Figure 4(C), Only 14 CMs are verified and 36 are unverified CMs. Here the cluster head ID is represented by 1 and from 2 to 51 are the IDs for CMs. The green on LED represent the verified CMs but off LED represents the unverified CMs.

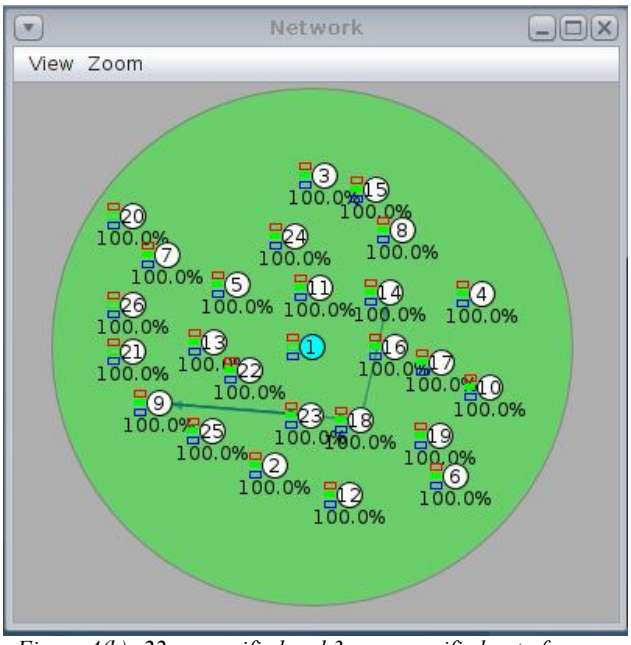

Figure 4(b): 22 are verified and 3 are unverified out of 25 CMs

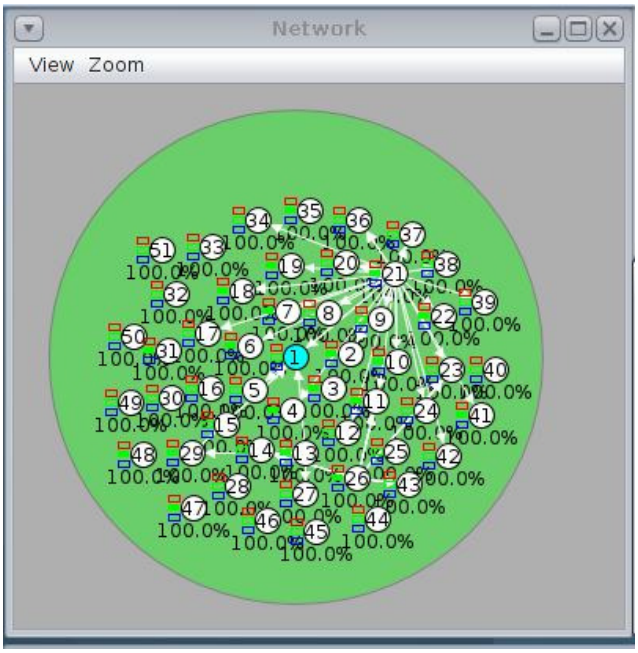

Figure 4(c): 14 are verified and 36 are unverified out of 50 CMs

Table 3: Drop Rate (Verified VS Unverified cluster members)

Number of CMs in a Cluster (Group)	Number of Verified CMs	Number of Unverified CMs
5	5	0
10	10	0

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

15	15	0
20	20	0
25	22	3
30	17	13
35	14	21
40	15	25
45	13	32
50	14	36

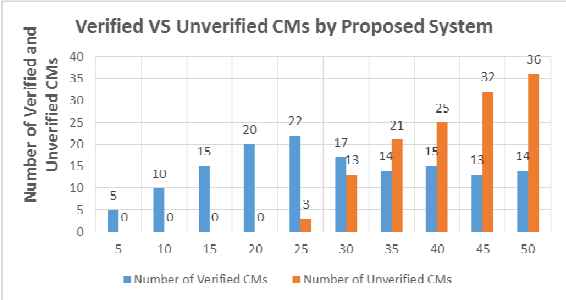

Figure 5(a): Verified VS Unverified CMs by Proposed System

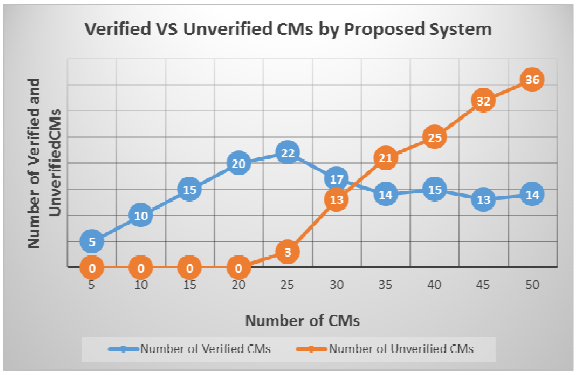

Figure 5(b): Verified VS Unverified CMs by Proposed System

8. CONCLUSION AND FUTURE WORK

This paper provides an overview of the WSN based conceptual model and its application towards smart crowd movement in the Internet of Things (IoT) paradigm. We discussed the model from perspective of verified and unverified (drop rate) CMs. We examined how the conceptual model work in simulation environment by using clustering and different operational phases. Explanation is done by use-case of the smart crowd movement.

If WSN based Smart Crowd Movement (Conceptual Model) is commercially implemented and deployed, it provides many application scenarios, such as:

i. To generate route planning of the crowd on the move.
ii. To generate alerts for deploying remote resources such as ambulances, water etc. in context of emergency situation of the crowd.
iii. To generate the shortest path to the incident location.
iv. Path finding in case of getting lost in mostly unknown territory.
v. Lost contact with cluster.
vi. Re-gathering plans with cluster.
vii. Generating the SOS calls in cases of real emergency situations. For examples: Sensing the level of the oxygen, if level is too low then generates the alert and give the direction where the level is better. In worst condition generate alert to medical emergency with current location (Sensor storage number). Sense the blood pressure and count heartbeat, if level is too low or high then generates the alert to the medical emergency with location.

This research shows some simulation results and on the base of simulation results, needs to be further expanded to test the WSN sensing emulation model into the laboratory and then in real environment. This is the one of the limitation that there is no such complete practically implemented model. The Internet and WSN communication causes dropping of packets due to low memory, less processing power and low energy. Therefore, factors affecting the packet dropping need to be identified and improved for efficient packet delivery. Furthermore, there is no such mechanism to identify that the person carrying the CM device is his own device or it has taken from another person (friend) or it has been stolen. In any case misplace or misuse of CM device causes a great risk in security view point.

REFRENCES:

[1] Memish ZA, Zumla A, Alhakeem RF, Assiri A, Turkestani A, Al Harby KD, Alyemni M, Dhafar K, Gautret P, Barbeschi M, McCloskey B. Hajj: infectious disease surveillance and control. The Lancet. 2014 Jun 20;383(9934):2073-82.

[2] Hassan SH, Zainal SR, Mohamed O. Determinants of Destination Knowledge Acquisition in Religious Tourism: Perspective of Umrah Travelers. International Journal of Marketing Studies. 2015 May 31;7(3):84.

[3] Waqas A, Mahessar AW, Mahmood N, Bhatti Z, Karbasi M, Shah A. Transaction Management Techniques and Practices In Current Cloud

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Computing Environments: A Survey. International Journal of Database Management Systems. 2015 Feb 1;7(1):41.

[4] Nesse PJ, Svaet SW, Strasunskas D, Gaivoronski AA. Assessment and optimisation of business opportunities for telecom operators in the cloud value network. Transactions on Emerging Telecommunications Technologies. 2013 Aug 1;24(5):503-16.

[5] Chourabi H, Nam T, Walker S, Gil-Garcia JR, Mellouli S, Nahon K, Pardo TA, Scholl HJ. Understanding smart cities: An integrative framework. InSystem Science (HICSS), 2012 45th Hawaii International Conference on 2012 Jan 4 (pp. 2289-2297). IEEE.

[6] Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the internet of things: A survey. IEEE Communications Surveys & Tutorials. 2014 Jan 1;16(1):414-54.

[7] Bandyopadhyay S, Coyle EJ. An energy efficient hierarchical clustering algorithm for wireless sensor networks. InINFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies 2003 Apr 3 (Vol. 3, pp. 1713-1723). IEEE.

[8] Nawaz NA, Waqas A, Yusof ZM, Shah A. WSN BASED SENSING MODEL FOR SMART CROWD MOVEMENT WITH IDENTIFICATION: A CONCEPTUAL MODEL. IADIS International Journal on Computer Science & Information Systems. 2016 Jul 1;11(2).

[9] Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Sensing as a service model for smart cities supported by internet of things. Transactions on Emerging Telecommunications Technologies. 2014 Jan 1;25(1):81-93.

[10] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Communications magazine. 2002 Aug;40(8):102-14.

[11] Higuchi T, Yamaguchi H, Higashino T, Takai M. A neighbor collaboration mechanism for mobile crowd sensing in opportunistic networks. InCommunications (ICC), 2014 IEEE International Conference on 2014 Jun 10 (pp. 42-47). IEEE.

[12] Zaslavsky A, Perera C, Georgakopoulos D. Sensing as a service and big data. arXiv preprint arXiv:1301.0159. 2013 Jan 2.

[13] Cabral Pinto F, Chainho P, Pássaro N, Santiago F, Corujo D, Gomes D. The business of things architecture. Transactions on emerging telecommunications technologies. 2013 Jun 1;24(4):441-52.

[14] Aly SA, Ali-Eldin A, Poor HV. A distributed data collection algorithm for wireless sensor networks with persistent storage nodes. InNew Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on 2011 Feb 7 (pp. 1-5). IEEE.

[15] Banerjee, P., Friedrich, R., Bash, C., Goldsack, P., Huberman, B., Manley, J., ... & Veitch, A. (2011). Everything as a service: Powering the new information economy. *Computer*, (3), 36-43.

[16] Rimal BP, Jukan A, Katsaros D, Goeleven Y. Architectural requirements for cloud computing systems: an enterprise cloud approach. Journal of Grid Computing. 2011 Mar 1;9(1):3-26.

[17] Aly SA. Distributed data collection and storage algorithms for collaborative learning vision sensor devices with applications to pilgrimage. International Journal of Sensor Networks. 2012 Jan 1;12(3):137-48.

[18] Whitmore A, Agarwal A, Da Xu L. The Internet of Things—A survey of topics and trends. Information Systems Frontiers. 2015 Apr 1;17(2):261-74.

[19] Da Xu L, He W, Li S. Internet of things in industries: A survey. IEEE Transactions on industrial informatics. 2014 Nov;10(4):2233-43.

[20] Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems. 2013 Sep 30;29(7):1645-60.

[21] Liaqat M, Chang V, Gani A, Hamid SH, Ali RL, Haseeb RM, Maqsood T. Towards Sensor-Cloud Integration: A Survey of Enabling Technologies and Architectures. International Journal of Information Management. 2016 May 28.

[22] Wigan MR, Clarke R. Big data's big unintended consequences. Computer. 2013 Jun;46(6):46-53.

[23] Krischkowsky A, Trösterer S, Bruckenberger U, Maurer B, Neureiter K, Perterer N, Baumgartner A, Meschtscherjakov A, Tscheligi M. The Impact of Spatial Properties on Collaboration: An Exploratory Study in the Automotive Domain. In Proceedings of the 19th International Conference on Supporting Group Work 2016 Nov 13 (pp. 245-255). ACM.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[24] Waqas A, Yusof ZM, Shah A, Bhatti Z, Mahmood N. Simulation of resource sharing architecture between clouds (ReSA) using Java programming. In Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on 2014 Nov 17 (pp. 1-6). IEEE.

[25] Waqas A, Yusof ZM, Shah A, Mahmood N. Sharing of attacks information across clouds for improving security: A conceptual framework. In Computer, Communications, and Control Technology (I4CT), 2014 International Conference on 2014 Sep 2 (pp. 255-260). IEEE.

[26] Waqas A, Yusof ZM, Shah A, Khan MA. ReSA: Architecture for resources sharing between clouds. In Information Assurance and Cyber Security (CIACS), 2014 Conference on 2014 Jun 12 (pp. 23-28). IEEE.

[27] Waqas A, Yusof ZM, Shah A. A security-based survey and classification of Cloud Architectures, State of Art and Future Directions. In Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on 2013 Dec 23 (pp. 284-289). IEEE.

[28] Waqas A, Yusof ZM, Shah A. Fault tolerant cloud auditing. In Information and Communication Technology for the Muslim World (ICT4M), 2013 5th International Conference on 2013 Mar 26 (pp. 1-5). IEEE.