Full/Regular Research Paper, CSCI-ISOT

An NFC Based Student Attendance Tracking/ Monitoring System Using an IoT Approach

Janea Dixon
Department of Computer Science and Engineering
University of Bridgeport
Bridgeport, CT, USA
jdixon@my.bridgeport.edu

Abdel-shakour Abuzneid
Department of Computer Science and Engineering
University of Bridgeport
Bridgeport, CT, USA
abuzneid@bridgeport.edu

***Abstract*—Student attendance shapes many aspects of a university; however, it's still widely recorded by hand. While it is common for a professor to pass around a sign-in sheet to enter in attendance to a web-based application later manually, this makes for an unreliable method, leaving many inconsistencies. With today's advances in technology, an automated attendance recording, tracking, and monitoring system will greatly improve the efficiency and reliability of attendance tracking. Several other works have proposed solutions using near field communication and IoT technologies; however, many use a single point at the start of a lecture to record attendance. This is likely to cause bottlenecks and take away time from the course. We implemented a system that incorporates NFC, cloud-based services, and a web interface for end-users. Our design introduces a one-to-one method using a student ID with an RFID tag to RFID reader located at each desk.**

Keywords— Internet of Things, IoT, NFC, RFID, Attendance Tracking

I. INTRODUCTION

Student attendance has a significant impact on their performance in each course. Students with a higher attendance rate, generally perform better than students who tend to be no shows. To combat this, professors often incorporate a maximum number of missed lectures into the syllabus. However, attendance tracking is most often done by hand, making it tedious, time consuming, and widely unreliable. After each class, the professor must manually update their record against the new list. While this may not take much time for a class size of twenty, a full lecture hall may provide more of a challenge. Aside from this, there is no guard against students writing in other names on the list to cover for their peers. Besides, if a professor misplaces the attendance sheet after taking attendance, there is no way to recover the information. For these reasons, some professors opt to skip attendance tracking altogether. In order for professors to accurately track which students are present in each lecture, implementing a reliable solution is necessary.

Over the last decade, the Internet of Things approach to update mundane tasks and provide solutions that are on par with today's technology has become commonplace. There have been significant advancements in communication devices and technologies that boost this practice to new levels[1]. An up-to-date attendance tracking and monitoring system is no exception.

Many studies have been done using various methods of implementation to create an attendance monitoring system that incorporates IoT technologies. Benyó et al. [2] developed and installed a system that uses terminals that have biometric authentication and nearfield communication identification tags. Though they present a strong idea for attendance tracking in a university setting, the system was implemented for a relatively small number of students. While this method may be effective for universities with small class sizes, it is not practical schools with medium to large student enrollments.

Other IoT methods for developing an effective attendance monitoring system include RFID technology using tags and mobile devices, biometric authentication, mobile or web-based user applications, and other communication technologies. Each approach contains similar ideas with varying approaches.

In this work, we aim to build upon previous studies to present an IoT based attendance tracking and monitoring system that is applicable to university use on a large scale. Our method includes RFID, specifically nearfield communication (NFC) readers and tags, IoT messaging with cloud-based device management, a database for storage, and a user web application. The proposed system will grant each student a secure student ID with an NFC tag. Each student will be able to record their attendance simply by tapping an NFC reader at the desk they have chosen to sit. This system is fully automatic. The professor can view attendance in the class at any time by accessing the web application. This approach removes the possibility of a bottleneck and allows attendance recording to be seamless and lectures are able to begin immediately.

The rest of the paper is organized as follows: section 2 discusses other related work on attendance tracking monitoring systems that use an IoT approach, section 3 details key technologies used in our proposed system, and section 4 explains the system architecture. Section 5 presents the implementation results, section 6 sheds light on possible future work that can be incorporated into this work, and finally, section 7 wraps up the paper with the conclusion.

978-1-7281-7624-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CSCI51800.2020.00201

II. Related work

Various studies have been done in the past to implement an IoT based solution to attendance monitoring and tracking that includes RFID/NFC. NFC is widely available in mobile devices today, making it a desirable tool to use to develop an attendance tracking system. Jacob et al. [3] propose a solution that uses NFC to identify a student combined with a one-time password (OTP) to authenticate. To initiate the attendance processes, the professor will open the android based attendance application, and each student will need to tap their NFC Tag/ID card on the phone. The student should then receive an SMS on their registered mobile device. The student must then, using the college WiFi, long into an online-based application and enter in the OTP to confirm attendance. Masruroh et al. [4] Created a mobile-based system that incorporates image captures to authenticate the student and web application to get a concise attendance report. The student, upon entering the course, must tap the NFC reader and standby to take a picture. The details are then saved to a database and displayed in the web application. While both of these solutions would successfully record attendance, the process is not practical for a classroom environment. Each student would need a working android phone present with them for each course. Also, it would likely become time-consuming, taking away from valuable lecture time.

Srinidhi et al. [5] designed a comprehensive system that includes an RFID student ID card and biometric authentication, as well as many different components and features. Each student must tap their ID card on the RFID reader and scan their fingerprint. The fingerprint is then sent to the server where it checks for a match in the database. If a match is found, then it marks the student as present. The attendance report can be viewed in both web and mobile applications. Benyó et al. [2] present a system with a similar workflow; however, they created terminals that will be positioned outside of the course rather than inside the class where it is only accessible for the first 5 minutes before and after the lecture begins. Also, the student's fingerprint is saved securely on the student ID card, and their fingerprint is scanned and matched at the terminal. Both systems present great solutions. Srinidhi et al. [5] included many useful features in their design, with the use of "hotspots" around campus being one of them. These hotspots can be used to live track the number of students in the same place. Students would be able to check crowds at an on-campus event or security can use them to monitor the number of people on campus at any given time. While this feature is a nice bonus, Benyó et al. [2] may be more practical and secure for attendance tracking since there is no time constraint, and the fingerprint templates are not stored in a database.

Many studies, including the works, discussed, all contain a single point failure. Each system relies on one reader. In a classroom environment, students and professors often show up late. Attendance systems should not be disruptive or take too much time out of a lecture. Having a single reader in front of the class may be time-consuming and draw attention away from the lecture when latecomers arrive. To combat this, some implement a time limit where if the student is not marked present within a specific amount of time, they are marked absent. However, this may cut off students at the end of the line, who arrived and are now waiting for their turn for attendance. For these reasons, many professors still favor passing around a sheet of paper to record attendance since it can be done quietly, without any crowding or distractions. We are proposing a fully automatic attendance tracking and monitoring system, using IoT to create a one-to-one solution between students and readers.

III. Key Technologies for Our Proposed Model

In this section, we describe two key technologies that are used in the implantation of our model.

A. Message Queuing Telemetry Transport (MQTT) Protocol

MQTT is a lightweight device to device/IoT connectivity protocol [6]. There are two types of network entities, a message broker and its clients. The message broker is responsible for receiving all messages, filtering them, and sending them to the appropriate clients. The clients are the devices that can connect to a broker and send/receive messages. This protocol allows for bidirectional communication and will enable devices to be controlled remotely.

In my model, the IoT Hub acts as the message broker, and the clients are the NFC reader devices. It filters all messages sent to it from the devices and stores the data into a database table. Since the number of new attendance records that would go into the database is likely to be thousands daily, using this service as a middleman is an optimal solution.

B. Near field Communication (NFC)

Nearfield Communication is a short-range wireless technology that allows communication between devices when they are touched together, or brought within a few centimeters of one another. It is specialized subset of RFID technology. It is convenient, has a low energy requirement, and does not require an authentication link between two devices [7].

NFC can be categorized as either full (active) NFC devices, where they are able to interact with their NFC peers, or as NFC tags where only passive data is stored to be read or written by full NFC devices. NFC operates in three different modes. The first is card emulator mode where it acts as a full NFC card that can be read by NFC devices [7]. The second, is NFC reader/writer mode where it can read and write to an NFC tag. Lastly, there is peer to peer mode where two full NFC devices can share data between each other. A smart phone is an example of a full NFC devices since it is capable of utilizing the all three NFC modes.

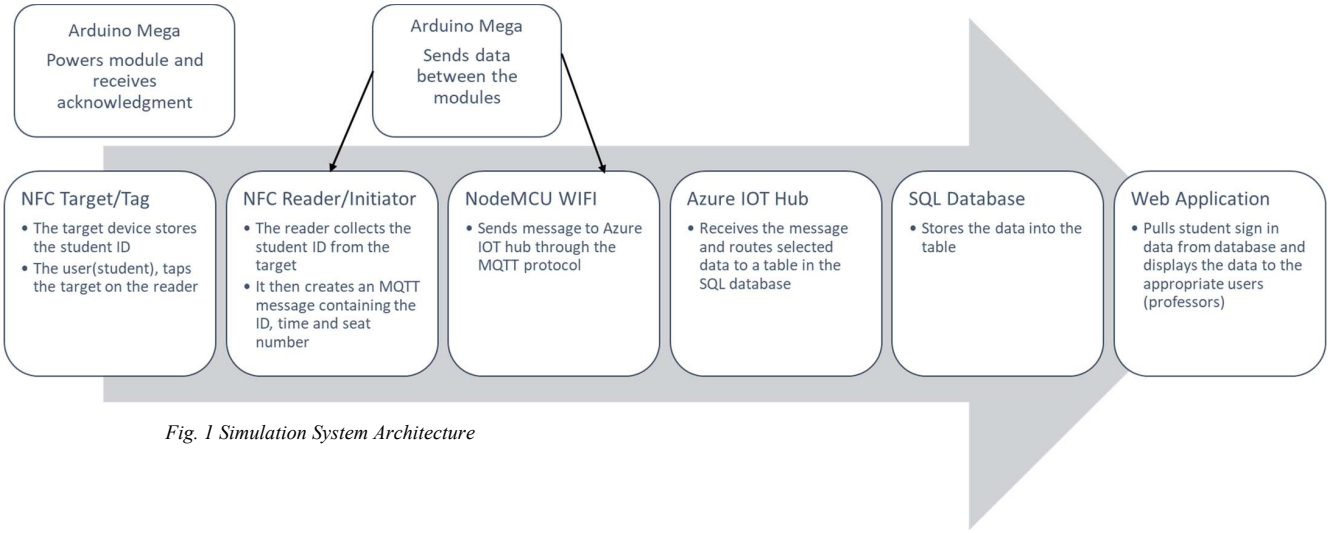


Fig. 1 Simulation System Architecture

In my proposed system, NFC is used in the student ID card and the reader device located on each desk. The NFC tag in the ID will hold the student's ID number. When a student taps the card on the reader, the reader parses the ID number and sends a message to the IoT Hub.

IV. System Architecture

A. Hardware System Architecture

1) NFC Student ID Card

A significant advancement in smart cards is their security. They contain a tamper-resistant chip that can run applications and store data [8]. They are also present in smartphones and used for fingerprint verification for NFC payments on mobile. Contactless cards must adhere to ISO/IEC 14443 standards. NXP's MIFARE protocol for contactless cards is the most dominantly used, followed by EMV standards for payment cards. NXP's Mifare DESFire EV1 and EV2 cards provide excellent speed and performance and security against a wide range of attacks because it can be implemented with DES two-key 3DES, three-key 3DES and AES encryption and is compliant on all four levels of ISO/IEC 14443A. Java cards or MUTOS are the most notable operating systems deployed on contact cards [8]. This is also due to their performance and security.

To simulate the NFC card, we used an Arduino Mega with a PN532 NFC module. The NFC module holds only the student ID number. When it comes within a few centimeters of the reader module, the Arduino will print "Target is sensed," and the student ID number is sent to the reader module. If the data transfer is successful, the reader will print a message that confirms the receipt of the ID number.

2) Desk with NFC reader, processing unit and WIFI

Smart objects are on the rise, with IoT being a major focal point. Smart desks and tables have been proposed in various works. As part of the architecture, I am proposing a wireless device with NFC reading capabilities be built into desks. This would allow each student to mark their attendance individually. The ID on the card will be read by the reader. The reader will send the ID number, and desk, to a cloud-based database. This would be the key to removing all delays that would occur for any system that proposes a single sign-in point at the start of each lecture.

In my model, I use an Arduino Mega for processing, PN532 NFC Module to read the student ID card and a NodeMCU to send IoT messages over WiFi. Messages are sent from the Arduino to the IoT hub using the MQTT protocol. The message contains various information to identify the student, course, and sign-in time.

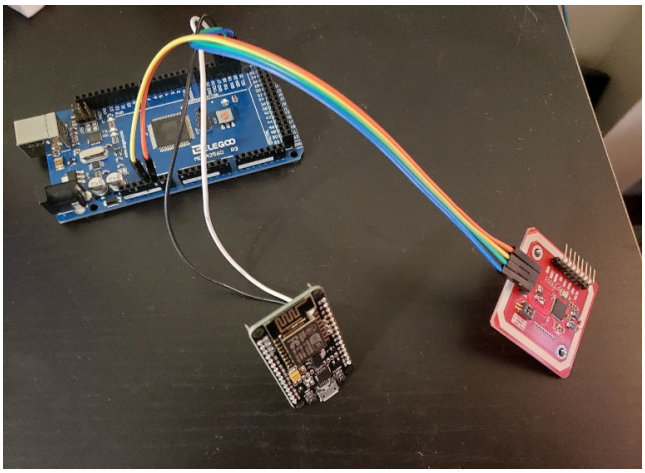


Fig. 2 Arduino with NFC reader and NodeMCU Wi-Fi Module

B. Software System Architecture

1) Cloud-Based Database

A database is needed to store each student's attendance record. The database consists of multiple tables that are accessed by a web application. Each record includes a student ID, seat number, sign in time, and a message ID. The student ID number and the sign-in time is crossed referenced with the student schedule to find which course the student is attempting

to sign into at the time. If there is no course scheduled for that time, the attendance is not saved. If there is, the record is inserted with a listing ID and a lecture ID. Each listing presents information regarding all courses offered in a particular semester. Each lecture ID is a single instance of a listing, with the specific date the lecture is offered.

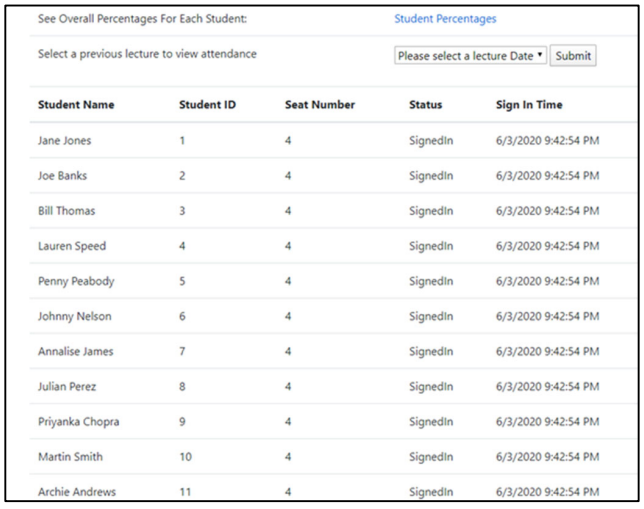
The database stores messages that are output from the Azure IoT HUB. In the model, we used SqlServer available on the Azure platform. This allowed for ease of use with many of the different services provided on the platform.

2) Azure IoT Hub

The IoT hub is a cloud service that acts as a middleman between an IoT application and the device or devices it controls. In our model, using Arduino with the WiFi module, we send messages to the IoT hub over the MQTT protocol. The IoT hub, using stream analytics, the messages are parsed and, if valid, stored into an SQL table. The hub can quickly sift through many messages. This is useful since many students with one or more courses will be signing regularly. This means thousands of messages daily. Using this hub is an excellent way to monitor data coming from the NFC Reader. Since it supports bi-directional communication, it sends back information and status to the reader device. This can be used to verify messages that have successfully sent.

3) Web Application

The web application is available for professors to view the attendance for each course they are teaching. The professor can view the current lecture and all past lectures. Each professor has an account where they can log into and see the attendance report. The application will provide a percentage of students who marked their attendance for each lecture and an overall rate for the course. The app also offers individual rates per student. The classes are updated by the registers department. Upon a professor login in, their current schedule is already populated.


See Overall Percentages For Each Student: Student Percentages

Select a previous lecture to view attendance: Please select a lecture Date | Submit

Student Name	Student ID	Seat Number	Status	Sign In Time
Jane Jones	1	4	SignedIn	6/3/2020 9:42:54 PM
Joe Banks	2	4	SignedIn	6/3/2020 9:42:54 PM
Bill Thomas	3	4	SignedIn	6/3/2020 9:42:54 PM
Lauren Speed	4	4	SignedIn	6/3/2020 9:42:54 PM
Penny Peabody	5	4	SignedIn	6/3/2020 9:42:54 PM
Johnny Nelson	6	4	SignedIn	6/3/2020 9:42:54 PM
Annalise James	7	4	SignedIn	6/3/2020 9:42:54 PM
Julian Perez	8	4	SignedIn	6/3/2020 9:42:54 PM
Priyanka Chopra	9	4	SignedIn	6/3/2020 9:42:54 PM
Martin Smith	10	4	SignedIn	6/3/2020 9:42:54 PM
Archie Andrews	11	4	SignedIn	6/3/2020 9:42:54 PM

Fig. 3 Web application showing students and sign in times

V. Implementation Results

We set up a prototype student ID card and model the NFC reader device. On the web application, we created several courses and enrolled 10 to 15 students in each class. The attendance recording is time and ID based. This means, only during the set course time will a student's attendance be saved into the database. For the test student, we tapped the NFC card to the reader device during scheduled course time. The reader sends out a message received confirmation before sending the student ID, seat number, and timestamp to the Azure IoT Hub via MQTT message. Using Azure analytics, the message is parsed and stored in a cloud-based SQL database. We then logged into the web application as the professor teaching the course. On the main page, it lists all the courses the professor is currently teaching. We selected the course that the student is registered in and then selected the lecture date. The page displayed the student has successfully recorded their attendance and the time it was recorded.

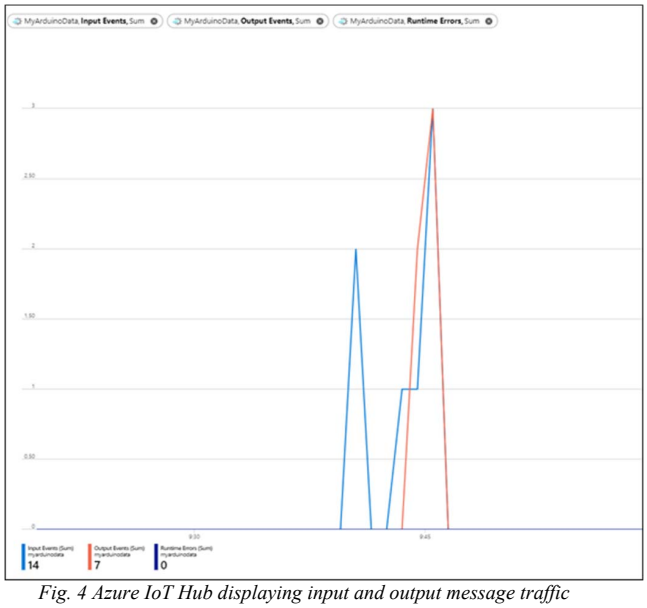


Fig. 4 Azure IoT Hub displaying input and output message traffic

For each lecture, the enrolled students are listed and their attendance status at that current point in time. To simulate varying numbers of students attending a specific course and lecture, we also set up a simulated device in C#. This device sends the same message to the IoT Hub as the reader device with different student ID's. This allowed us to observe lectures with 100 percent attendance displayed on the web application.

VI. Future Work

Studies for a practical IoT approach to attendance tracking and monitoring will continue to grow as technology continues to advance. With advances come new cybersecurity risks. We must consider the possible attacks and safety of our information. Future implementations can include biometric authentication with a pin or security question as a backup. This

would ensure that each student is who they say they are and remove the possibility of someone else recording their attendance in their place.

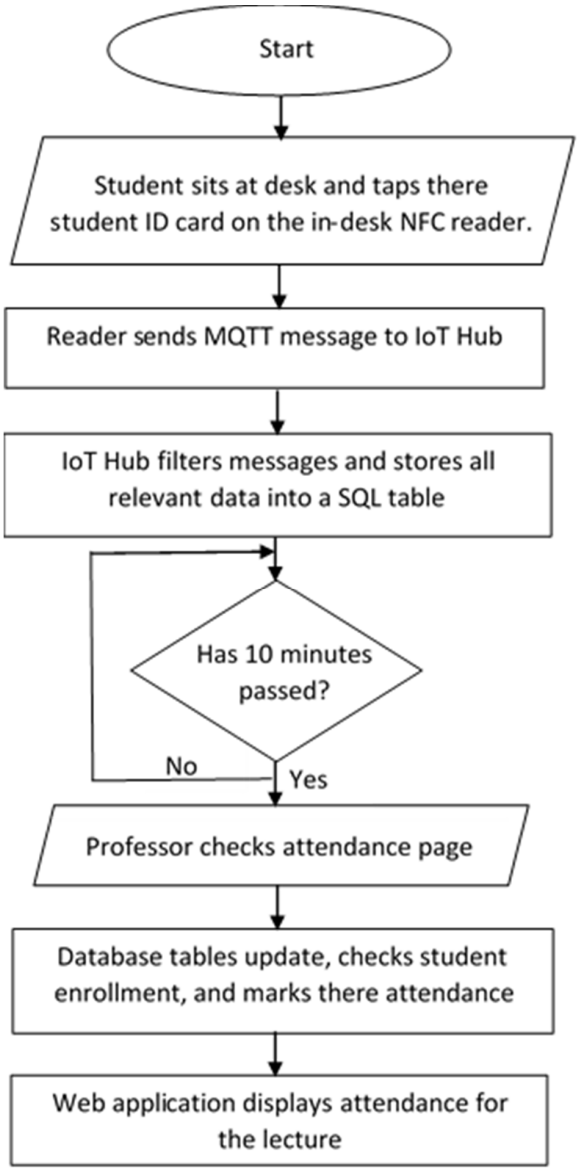


Fig. 5 System architecture flowchart

VII. Conclusion

In this paper, we proposed an attendance tracking monitoring system that utilizes RFID and other IoT technologies. Our implementation was successful in recording student attendance using our models. The NFC reader extracted the student ID from the NFC tag and sent it to the database over WiFi. We were then able to view the record in the web application.

In many similar studies, they present reasonable ideas in their work; however, many provide no solution to the possibility of a bottleneck. Our proposed system removes the prospect of this occurring and creates an environment where attendance taking is simple, quick, convenient, and distraction-less.

VIII. References

[1] S. N. Shah and A. Abuzneid, "IoT Based Smart Attendance System (SAS) Using RFID," in *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 3-3 May 2019 2019, pp. 1-6, doi: 10.1109/LISAT.2019.8817339.

[2] B. Benyó, B. Sódor, T. Doktor, and G. Fördős, "Student attendance monitoring at the university using NFC," in *Wireless Telecommunications Symposium 2012*, 18-20 April 2012 2012, pp. 1-5, doi: 10.1109/WTS.2012.6266137.

[3] J. Jacob, K. Jha, P. Kotak, and S. Puthran, "Mobile attendance using Near Field Communication and One-Time Password," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 8-10 Oct. 2015 2015, pp. 1298-1303, doi: 10.1109/ICGCIoT.2015.7380666.

[4] S. U. Masruroh, A. Fiade, and I. R. Julia, "NFC Based Mobile Attendence System with Facial Authorization on Raspberry Pi and Cloud Server," in *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 7-9 Aug. 2018 2018, pp. 1-6, doi: 10.1109/CITSM.2018.8674293.

[5] M. B. Srinidhi and R. Roy, "A web enabled secured system for attendance monitoring and real time location tracking using Biometric and Radio Frequency Identification (RFID) technology," in *2015 International Conference on Computer Communication and Informatics (ICCCI)*, 8-10 Jan. 2015 2015, pp. 1-5, doi: 10.1109/ICCCI.2015.7218103.

[6] O. Sadio, I. Ngom, and C. Lishou, "Lightweight Security Scheme for MQTT/MQTT-SN Protocol," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 22-25 Oct. 2019 2019, pp. 119-123, doi: 10.1109/IOTSMS48152.2019.8939177.

[7] C. Bermejo and P. Hui, "Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags," 05/05 2017.

[8] D. Sethia, D. Gupta, T. Mittal, U. Arora, and H. Saran, "NFC based secure mobile healthcare system," in *2014 Sixth International Conference on Communication Systems and Networks (COMSNETS)*, 6-10 Jan. 2014 2014, pp. 1-6, doi: 10.1109/COMSNETS.2014.6734919.