Received 24 October 2020; Accepted 15 December 2020.

Detection of SMS Fraudulent using ANN Algorithm.

Dr. Sachin Chaudhari[1], Ankita Kamthe[2], Mayuri Kudmethe [3], Neha Barapatre [4], Simran Bahenwar [5]

1 Associate Professor, Computer Science & Engineering Department, RTMNU University, Jhulelal Institute of Technology Nagpur, Maharashtra, India
2,3,4,5 Student, Computer Science & Engineering Department, RTMNU University, Jhulelal Institute of Technology Nagpur, Maharashtra, India

Abstract

Phishing, for example, Deceitful fraud is perhaps the most hazardous strategy for social designing to overcome end-clients when compromising characters access touchy data, for example, Mastercard subtleties, usernames, and passwords. It is one of all the social designing strategies that accumulate individual data through sites or email correspondence with an inserted hyperlink. Phishing frequently assaults email by utilizing it as a vehicle and in any event, sending messages by email to clients that address a part of an association who perform professional banking and so on In this paper, here present Phish Limiter, another procurement technique, whereinto propose another inside and out bundle testing (DPI) cycle and execute it through network-characterized organizing. (SDN) to spot phishing exercises through SMS and email. On the web, misrepresentation urges analysts to foster a model that can concoct greater security as far as the security administrations offered on the net.
Sources with crime police headquarters said they received over ten written complaints on radiotelephone malware attacks until Mon, with the victims claiming to own lost cash from their bank accounts. “The SMSs seem like regular text messages sent by banks. However, they're sent by fraudsters and contain a link. All the complainants clicked on the link, that resulted in an exceedingly malware incursive their phone, via that the conmen gained access to the device and every one SMSs received by the user,” discovered Associate in Nursing work officer inquisitory the fraud. They target folks whose bank credentials area unit already in their possession, police same. Investigators believe that when causing the texts, scamsters entered the users’ on-line banking interface and generated OTPs to draw cash from the complainants’ bank accounts. “As so much as phone banking frauds area unit involved, this can be one step prior to vishing, wherever crooks cause as bank executives and raise to the customer’s click on the hyperlinks gift within the messages and supply the PIN. The new malware is a straightforward tool and a secret weapon to steal cash from bank accounts,” the officer supplemental.
This paper shows various results of SMS phishing fraud detection using ANN and SDN algorithm, and the result are also discussed.

Keywords: Network-defined networking (SDN), Artificial Neural Network (ANN), Phishing.

1. Introduction

In the cyber world, from the past couple of decade phishing become one the most common and deadly attacks. Phishing has been reported first in the America in 1995. Phishing is mechanism of employing both social engineering and technical tricks to steal someone’s personal information like passwords, ATM pin etc. A message send by threat
attacker is commonly known as phishing. In phishing the attacker sent an e-mail to the end user or the text message, after that the attacker waits for the end user to click on the LINK sent by the attacker so that the link can extract all the sensitive information from the end user’s device.

Globally, phishing attacks were growing tremendously by 65%. The main aim of the phishing for attacker is to gather all the sensitive information like passwords, username, ATM pins, bank accounts credentials, without any information. There are different types of cybercrime but phishing is one of the most common and dangerous.

The attacker, who wants to extract sensitive information from the end users first they create the almost exact replica of the real website of the company that deals with financial information. They also use fake phone numbers to send the links not just e-mail. The main purpose for the replica website is that the Internet has grown so rapidly as a communication medium because of the logo and name of the company, they immediately want to open that link. Phisher then send the spoofed text to as many people as possible to coax them into the false scheme. When the people click on that link, the person or the end user redirected to the spoofed website and then they fill all the sensitive information in the spoofed website by doing this all the information get extracted without any clue by that attacker.

The use of an IDS (Intrusion Detection System) heavily depends on the response time of the detection mechanism to determine adverse behaviours Worrying about such a response time is when the user clicks on a link that leads to system crashes before the warning is added for further reduction attempts using an IPS (Intrusion Prevention System).

The technology used for the proposed project is ANN (Artificial Neural Network). Artificial Neural Network(ANN) uses the process of the brain as a basis to develop algorithms which will be accustomed model complicated patterns are used for detection prediction of insecure linksand SDN (Software- Defined Network). The human brain interprets the context of real world conditions in a way that computers cannot. The neural artificial network (ANN) is an attempt to mimic the sensory network that builds the human brain so that the computer can read things and make decisions the way human brain does. If to want ANNs to learn something then it need to send massive amount of information to them called a training set. When we try to teach ANN how to separate a cat and a dog, the training set will provide thousands of pictures marked as a dog network would begin to learn. Once we done teaching that, we will validate that if the machine’s output is correct or not. If YES then we successfully taught machine difference between dog and cat if not then it failed.

Network-defined networking (SDN) is a structure designed to make the network more flexible and easy to manage. SDN focuses on management by deploying control aircraft in the process of transferring data to different communication devices. SDN is also used in the traffic management of the network.

2. Literature Survey

In several businesses consider that text messages are more effective than e-mails. This is because 82% of SMSs are read within 5 minutes, but consumers open only one of the four emails they receive. The importance of SMS for mobile phone users has attracted the attention of spammers. [1] The volume of SMS spam has increased considerably in recent years with the emergence of new security threats, such as Phishing.

In modern years, the fame of cell phone gadgets has expanded; Short Message Service (SMS) has developed into a multi-billion dollars business. SMS spams are one of the concerns and a lot of individuals do not like to accept them as they are annoying. Many SMS spam detection methods already exist as well as various separators such as the Support Vector machine. [2] SMS spam detection system is proposed to identify an efficient set of features using Restricted Boltzmann Machine (RBM), a deep learning approach.

During Internet Banking, most people would hear the term “Crime Theft of Sensitive Information”, related to Internet fraud as well as Social Engineering. It is usually done by sending an email to identify the user with an embedded link to steal their username, password, transaction password, etc. [3] Phishers are used to gain access to the identity of the intended user's identity by stealing money from the user's bank account. The crime of stealing sensitive information are often done through other means like texting (called “Smishing” for SMS-Phishing), or by making phone calls (often called “Vishing” for Voice-Phishing) or sometimes through social media itself including sending e - mail to a user or organization.

Phishing may be a fraudulent attempt by cybercriminals, where the audience is addressed by a text message, call or e-mail. [4] Attacks on sensitive identity theft can lead to financial loss and identity theft. To shield internet users from phishing attacks, numerous anti-phishing models have been proposed.

In recent years, there has been considerable interest among people to use short message service (SMS) as one of the essential and straightforward communications services on mobile devices. Increasing popularity of this service has also increased the number of attacks on mobile devices such as spam SMS messages. We proposed a completely unique machine learning method [5] for detection of SMS spam messages.

3. Proposed System

The proposed project is going to linked with the TEXT message app of the phone, when the receiver or the end user receives any text message that contains the URL then the receiver is going to be notified by the purposed system that if the link is fake or not. We have to apply the link validation for the application because android application link are the special types of links that allows the website URLs to immediately open the corresponding content in the android application without require user to select any particular application. To add link to the app, intent filters are used that opens purposed app content using the HTTP URLs which afterwards verify that the user owns (verified) both the application and the website URL. We have to find that the link is http or HTTPS, if the link is HTTPS then the is link is secure but if that link is not HTTPS then there is a good chance of stealing the sensitive information from the mobile phone, so we recommend to install the app in the phone. In the purposed system we applied the SSL (Secure sockets layer) validation to secure the end user information, in the purposed project we used SSL checkers to give security to the end user, after this the sensitive information of the end user couldn't be extracted. Cross Site scripting (XXS Engine) has also been used to alert the user that the link user already clicked is valid or not if the link is valid then the green sign will appear or else the danger sign will appear with red color.

XML (Extensible Markup Language) language is used to design the complete user interface. This is the most common language use for Android Studio. JAVA is used for the backend of the proposed project. Java allows you to write down the code once and run it anywhere on any platform (Windows, Mac OS, and Linux), making it an ideal choice for mobile application. We created dashboard and all the things which could not be directly accessed by the user. MySQL is used for the database to manage all the data which is going to be stored in it. The cloud server is also used to host the file. XSS Engine (Cross-site scripting) is a type of computer security risk that is more prevalent in web applications and enables attackers to insert third party content into web pages viewed by other users.
Android Studio is used as a tool in the propopsed system. Android Studio is that the official integrated development site (IDE) of Google's Google app, built on JetBrains' Intellij IDEA software and specifically designed for Android development. It replaces Eclipse Android Development Tools because the primary IDE for Android application development.

ANN and SDN algorithms are used in the proposed system whereas SDN is an emerging networking structure that aims to overcome limitations of legacy networks. The centralized management of SDN guarantees consistent policy enforcement, better scalability, holistic visibility and flex programmable network function. Includes global network planning and viewing of cybercrime attacks. SDN is also used in the traffic management of the network. And the proposed ANN model provides the best average accuracy of 98.39% compared to J48, SVM, Logistic regression and NaiveBayes. Therefore, in our android application, ANN model is used as an classifier.

In the system, the innovation is to apply the SSL validation to secure the information of the user. In the proposed project we used SSL checkers to give the security to user. In our system, we alert the user that the given message is valid or not. Also, cross site scripting (XSS engine) is there in the proposed system as an innovation.

4. Modules

Here we have Three major modules in our system application and database which are as describe below:-

4.1 LoginPage:In our android application, we developed a sign-in/register application. To keep it short and simple we checked if the username and email are unique during registration. In our system, we will checked whether the email field is empty or not. If it is, we will call the login function in the PHP script, else we will go to the registration function. In the system we used the function to create a Hash string of the password. To checked email address is a valid we had implemented a isValidEmail() method.

When the REGISTER button is clicked, our system will programmatically hide the SIGN IN button and display the EMAIL address input text field instead. The AttemptLogin class executes the network HTTP requests to our localhost in the background. The username, password and email parameters are added to an array list that are passed in the method.

4.2 Message abstraction: In our proposed android application, we used the method where we display the message string returned from the server in a Toast message. Here we called the respective classes i.e. post and get which depends on the second parameter passed in the method. We appending the response status code returned from the server in the final object that's returned to the MainActivity class. (ref. Figure 1)

Received 24 October 2020; Accepted 15 December 2020.

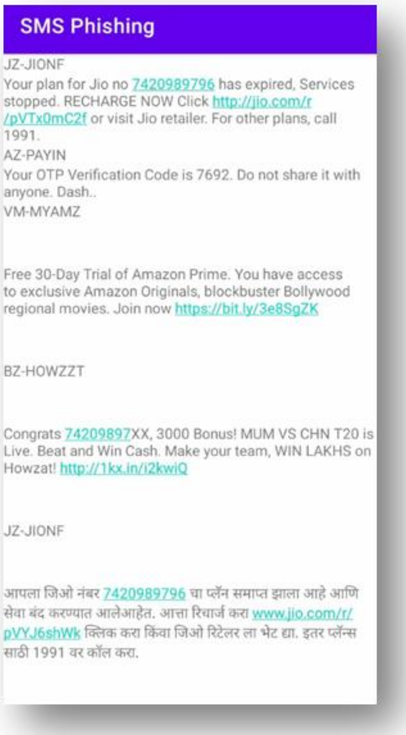
4.3 Server establishment: After clicking on the link in the message, we found that the link is secure or insecure using the algorithms like ANN Classifier and SDN algorithm. Here we abstract the feature from the link present in the message to predict the link is secure or insecure. If the link is invalid then to provide the security we established the torque browser server by clicking on the CONNECT button. If the link is secure its directly gets opened in the browser. (ref. Figure 2, 3, 4, 5)

- DATABASE: In our system, to create the backend server used XAMMP and MySQL database. XAMPP is a one-click installer software that creates an environment for developing a PHP, MySQL web application. Now test phpMyAdmin in the localhost. To sets the MySQL database open phpMyAdmin and then select the databases tab that's present in the top left of the headers row. In the proposed application, we used 'ID', 'USERNAME','PASSWORD'. To connect a PHP script to MySQL databases three inputs values are required that is 'HOST NAME', 'MySQL user name' and 'MySQL password'. In our system, we used PHP's inbuilt function to connect to MySQL database with the parameters. (ref. Figure 6)

5. Algorithm

```
Step 1: Start.
Step 2: User user permissions read-only sms.
Step 3: Fetch the link.
Step 4: If Link start with HTTP (HTTP stands for hypertext transfer protocol).
            Then show insecure connection
              Else
        If Link start with HTTPS (HTTPS stands for hypertext transfer protocol Secure).
        Then show secure connection.
Step 5: Stop.
```

6. Result



SMS Phishing

JZ-JIONF

Your plan for Jio no 7420989796 has expired, Services stopped. RECHARGE NOW Click http://jio.com/r/pVTx0mC2f or visit Jio retailer. For other plans, call 1991.

AZ-PAYIN

Your OTP Verification Code is 7692. Do not share it with anyone. Dash..

VM-MYAMZ

Free 30-Day Trial of Amazon Prime. You have access to exclusive Amazon Originals, blockbuster Bollywood regional movies. Join now https://bit.ly/3e8SgZK

BZ-HOWZZT

Congrats 74209897XX, 3000 Bonus! MUM VS CHN T20 is Live. Beat and Win Cash. Make your team, WIN LAKHS on Howzat! http://1kx.in/i2kwiQ

JZ-JIONF

आपला जिओ नंबर 7420989796 चा प्लॅन समाप्त झाला आहे आणि सेवा बंद करण्यात आलेआहेत. आत्ता रिचार्ज करा www.jio.com/r/pVYJ6shWk क्लिक करा किंवा जिओ रिटेलर ला भेट द्या. इतर प्लॅन्स साठी 1991 वर कॉल करा.

Figure 1. SMS Fetching Page of user's phone.

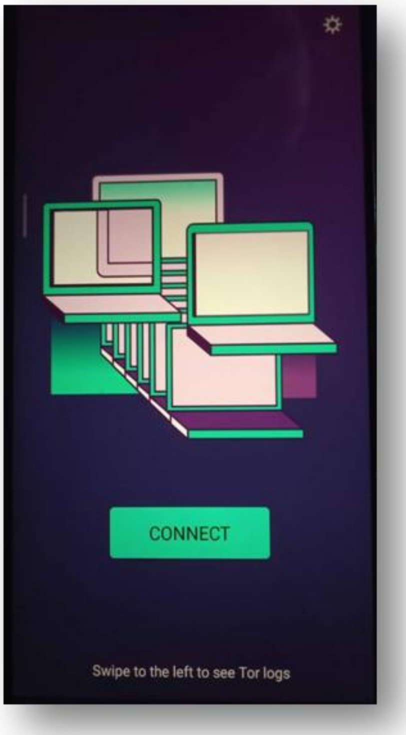
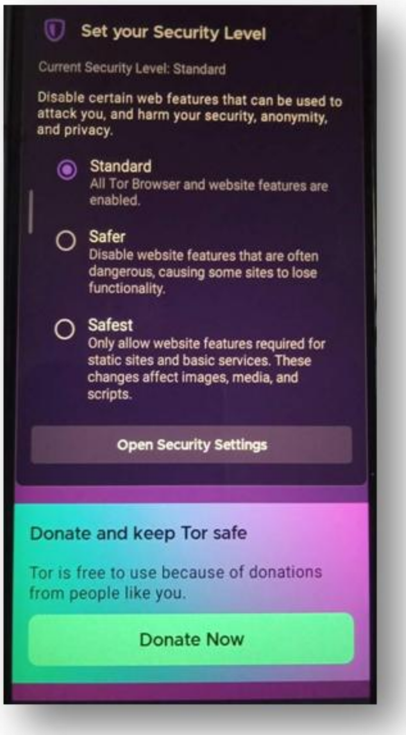


Figure 2. Tor browser Page (generated after connection establishment)



Set your Security Level

Current Security Level: Standard

Disable certain web features that can be used to attack you, and harm your security, anonymity, and privacy.

● Standard
All Tor Browser and website features are enabled.

○ Safer
Disable website features that are often dangerous, causing some sites to lose functionality.

○ Safest
Only allow website features required for static sites and basic services. These changes affect images, media, and scripts.

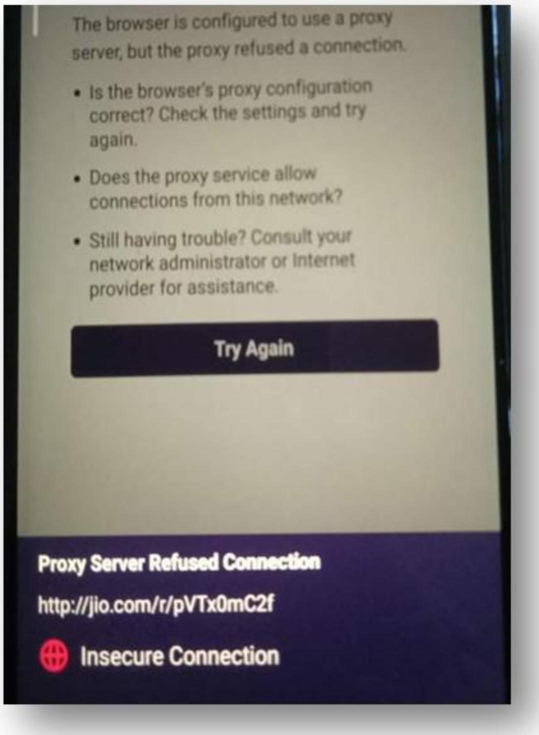
Open Security Settings

Donate and keep Tor safe

Tor is free to use because of donations from people like you.

Donate Now

Figure 3. Security Level Setting Page



The browser is configured to use a proxy server, but the proxy refused a connection.

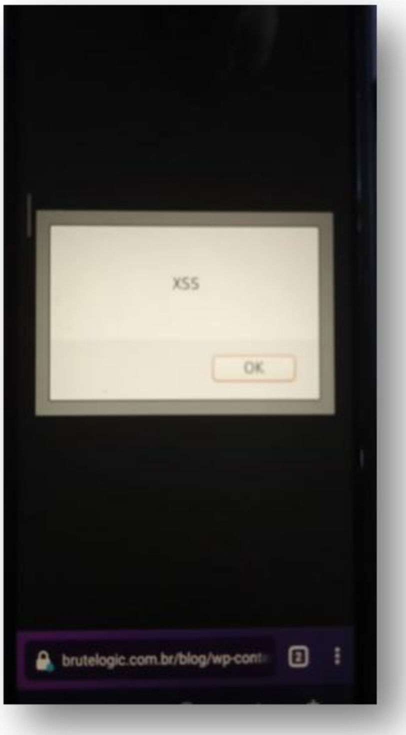
- Is the browser's proxy configuration correct? Check the settings and try again.
- Does the proxy service allow connections from this network?
- Still having trouble? Consult your network administrator or Internet provider for assistance.

Proxy Server Refused Connection

http://jio.com/r/pVTx0mC2f

Insecure Connection

Figure 4. Proxy Server Connection Checking Page



XSS

Figure 5. XSS (Cross-site scripting) Checking Page

Received 24 October 2020; Accepted 15 December 2020.

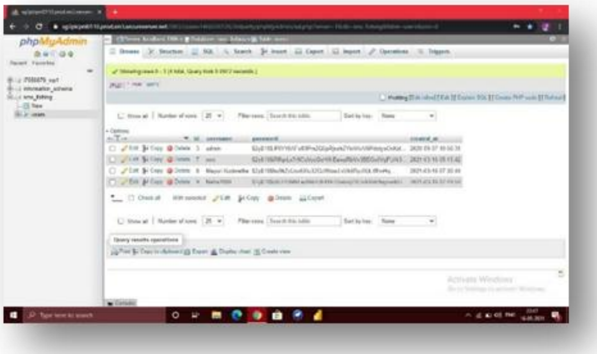


Figure 6. Database Page(php Admin)

7. Advantages

- The first and foremost benefit of the proposed is the decreased security risks of the end user due to social engineering attacks involving human manipulation and deception.
- It takes less mitigation time and manages traffic smoothly.
- The proposed system provides the security to the user about their information.
- Fast, less consuming memory, high accuracy, evolving with time.

8. Conclusions

Phishing attacks become most typical attacks nowadays targeting organization and also the user which is extremely harmful nowadays. During this paper, we demonstrated that there are such a lot of studies on detecting the phishing attack but the oldest technique for the answer of this can be proxy service supported static string matching in traditional IDS like SNORT and BRO. This purposed project has a capability to handle the network traffic dynamics and it's a worldwide view of networks because of SDN and handles the harmful phishing threat and ready to stop stealing the user’s sensitive information by the suspicious cyber criminals. Here we have attached our project working screenshots, which are as follows below

9. References

1. P. Prakash; M. Kumar; R. R. Kompella; M.
2. Gupta, ‘‘PhishNet: Predictive blacklisting to detect phishing attacks,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 – 5.
3. A. Blum; B. Wardman; T. Solorio; noG. Warner, ‘‘ Lexical feature based phishing URL detection using online learning, ’’ in Proc. 3 ACM Workshop Artif. Intell. Secur., 2010, pages 54-60.
4. S. Marchal; J. François; R. State; T. Engel, ‘‘Active availability of domain names related to the crime of identity theft, ’’ Proc. Int. Recent Workshop Adv. Access Access.
5. Berlin, Germany: Springer, 2012, pages 190– 209.S. Marchal, J. François, R. State, and T. Engel, ‘‘Proactive discovery of phishing related domain names,’’ in Proc. Int. Workshop Recent Adv. Intrusion Detection. Berlin, Germany: Springer, 2012, pp. 190– 209.
6. Barracuda. (2017). Barracuda Email Security Gateway. [Online]. Available: https://www.barracuda.com/products/emails ecuritygateway.
7. Symantec. (2017). Symantec Messaging Gateway. [Online]. Available: https://www.symantec.com/products/threatp rotection/messaginggateway
8. T. Chin; K. Xiong; M. Rahouti, ‘‘SDN-based kernel modular countermeasure for intrusion detection,’’ in Proc. 13th Int. Conf. Secur. Privacy Commun. Netw. Springer, 2017.
9. [Online]. Available: https://www.springer.com/us/book/9783319788128
10. A. Vahdat; D. Clark; J. Rexford, ‘‘A purpose– built global network: Google’s move to SDN,’’ Networks, vol. 13, no. 8, p. 100, 2015.
11. A. V. Akella; K. Xiong, ‘‘Quality of service (QoS)-guaranteed network resource allocation via software defined networking (SDN),’’ in Proc. IEEE 12th Int. Conf. Dependable, Auton. Secure Comput. (DASC), Aug. 2014, pp. 7–13.

12. B. Pfaff et al., “The design and implementation of open vSwitch,’’ in Proc. 12th USENIX Symp. Netw. Syst. Des. Implement. (NSDI), 2015, pp. 117–130.
13. Apache. (2017). Apache Spam Assassin Public Corpus. [Online]. Available: https://spamassassin.apache.org/publiccorpus/
14. Joo; J.W. Moon; S.Y. Singh; S. and Park; J.H. “Sdetector: an enhanced security model for detecting smishing attack for mobile computing.” Telecommun. Syst., 66, 1–10, 2017.
15. Rao, J. Nageswara, and M. Ramesh. "A Review on Data Mining & Big Data." Machine Learning Techniques. Int. J. Recent Technol. Eng 7 (2019): 914-916.
16. D. Veeraiah and J. N. Rao, "An Efficient Data Duplication System based on Hadoop Distributed File System," *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 197-200, doi: 10.1109/ICICT48043.2020.9112567.
17. D.R.V.A.Sharath Kumar, Y.Nagalakshmi and G.Sahithi, presented the paper in the International Conference on “Asynchronous techniques in Nano technology” at Sreenidhi Institute of Technology and Science, Hyderabad on January 2012.
18. A.K. Jain; B B Gupta; “Rule-based framework for detection of smishing messages in mobile environment”, Procedia Computer Science 125 (617– 623), 2018.
19. G. SonowalNoK. S. Kuppusamy, “SmiDCA: An anti-smishing model with machine learning approach”, the pc Journal, Vol 61, Issue 8, 2018,1143–1157.
20. D. Goel; A. K. Jain, “Smishing-classifier: a novel framework of detection of smishing attack in mobile”, NGCT 2017, CCIS 828, pages 502-512, 2018.
21. Jain Ankit ; Gupta B B "A method based on the feature of smoking messages in a portable environment".
22. S. N. Ajani and S. Y. Amdani, "Probabilistic path planning using current obstacle position in static environment," 2nd International Conference on Data, Engineering and Applications (IDEA), 2020, pp. 1-6, doi: 10.1109/IDEA49133.2020.9170727.
23. S. Ajani and M. Wanjari, "An Efficient Approach for Clustering Uncertain Data Mining Based on Hash Indexing and Voronoi Clustering," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 486-490, doi: 10.1109/CICN.2013.106.