ISSN Application No. 21726

Global Journal of Computer and Internet Security

Volume No. 11

Issue No. 1

January - April 2023

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

ISSN Application No. 21726

Global Journal of Computer and Internet Security

Aims and Scope

The Journal of Computer and Internet Security presents research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems. It also provides a forum for ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community.

ISSN Application No. 21726

Global Journal of Computer and Internet Security

(Volume No. 11, Issue No. 1, January - April 2023)

Contents

ISSN Application No. 21726

WSNs Prone to Swap Attacking and Eavesdropping

Shafiqul Abidin
HMRITM (Affiliated with GGSI P University),
Delhi, India

A B S T R A C T

This paper evaluates the nature and impact of Swap Attack and Eavesdropping in Wireless Sensor Network (WSNs). This shows the phenomenon of how it works at the industrial site which consists of a sink node and also contains multiple and are used in broadcasting of propagation of radio waves, the transmission from the sensor to the sink and from the sensor to the eavesdropper and the difference between these two is the secrecy capacity of the transmission through wireless mode. The transmitted data will be easily intercepted by an eavesdropper if the result or the secrecy capacity will be low or under positive or non negative resulting in the sense due to wireless fading effects as such as obstacles in machinery parts or vibrations through engines. Earlier, cryptographic techniques were used to save or prevent the coded information from eavesdropper having low computing capability but now the information can be decoded easily by the eavesdropper with having high computational capability. As such in Wireless Sensor Networks, the swap attack against Directed Diffusion, in this there are basically two nodes to be considered namely called as source node and sink node. The source node to be known from where the data are to be sent to other node and other node called as sink node where data are received. The Swap Attack works under the bad route for routing the messages. There are two modes called Norm mode and Halt mode through which swap attack is being performed whereas, in Norm mode the attacker node gets alternated between the bad and good routes in the on and off cycles whereas, in Halt mode, the attacker node can hide its Presence by putting itself in the sleep mode.

Keywords: Wireless Sensor Networks sensors, (WSNs); Swap Attack; Eavesdropping in WSN; Cryptography Techniques.

1. INTRODUCTION

The main application of Wireless Sensor Networks(WSNs) is that it is used in the army lines mainly in the surveillance [1] of battlefield and also the of this is major contributed to the industrial applications that is used in the factory efficiency from where the productivity [2] can be increased and hence results in the profit of the industry. For the purpose of use of industrial purpose it is often known as the industrial WSNs [3] and the distributed sensors in the industry results in the increment of the security purposes in the industry. The vibrations through machinery parts and engines are not good for the propagation of radio waves and causes severe damage to the work of transmission through wireless medium, which results in failure of security and machinery parts in turn will not work accordingly or properly and may in turn can cause harm to the lives of the workers working on the machines and can even result in disablement [4]. Working for WSNs at the industrial site, if it would be Wired Sensor Network not the wireless network, then there would be very less chance for the eavesdropper or for the eavesdropping attack in wired network than in comparison to the wireless network for the eavesdropper

because of its broadcast nature of radio waves for its propagation as such this is used in wireless network as this is not used in wired network so less chance for intercept by the eaves- dropper. It is important to make protection of the industrial WSNs as the eavesdropper can overheard the transmission through the transmission medium that is wireless medium from the sensors' information communication [5]. By the use of cryptography, the eavesdropper can decode the information and to reduce this the new technology called as physical layer security for the security purpose from eavesdropper are to be introduced.

For the swap attack, Directed Diffusion is used in which there are basically two nodes called source node and the sink node. In the source node, the data or the query is sent to the other nodes and the node that receives the information are said to be the sink node, which takes the information. The interest is created by the sink by using naming in this protocol. The messages are being sent to the all nodes according to the interest through the broadcasting periodically from the network. The interest cache is being created by receiving interest to the nodes from which stores all the interests and gradient values which determines the data rate and tells about the direction about the data flow. Interest caches are being checked by the source node to verify that more data is to be required or not. If the interest exists in the interest cache then data message are sent through gradient list from the sink at the highest possible data rate. The messages are being dropped if no match was found, by the source node. If the match was found and hence there will be no data in the data Cache then update of cache will be done through the source node otherwise the message will be drop by the source node. Gradient paths are established in the network by the messages which are sent from the sink node. The messages sent from the sink nodes directly proportional to the data rate which results in the data can be negative or positive.

2. BACKGROUND STUDY

Earlier cryptography techniques were used to protect the communications through wireless medium from the eavesdropper. But, as the hacking is increasing day by day and with the aid of attack known as brute force attack[6],[7] and with high computing power, the eavesdropper can be able to easily crack or decode the encrypted data. To work for security purpose or for securing communications, physical layer security [8] was introduced. The difference between the main link from the source to end point of the channel capacity and to that of wiretap link from the source point to the eavesdropper is called secrecy capacity [9]. If this would be increased then it would be difficult for the eavesdropper to intercepts the message. This would be the great limitation of the Wireless Network. By the use of artificial noise, it helps in improving the secrecy capacity and the receiver gets not affected. [10] this results in the increase of Secrecy capacity, without having any effect of the channel capacity. For the link to be not effected, the number of antennas should be more at the legitimate transmitter then that at the receiver [11].

As artificial noise increase secrecy capacity, but for this it also requires additional power cost. For this purpose, a multiuser scheduling scheme was introduced for Wireless security improvements of the networks, without any power cost[12]. For saving power resource and also for reducing complexity of the system, sensor scheduling is introduced. For security enhancement, the relay node has the highest secrecy in against of the eavesdroppers; in relay nodes the additional network nodes are introduced [13]. Also in the addition to this, artificially noise methods ,a great strategy was made in order to improve the security through wireless medium for distracting the mind of eavesdropper without affecting the destination source. The main topics covered or summarize of the contributions in this paper are the sensor scheduling scheme was introduced for securing data from eavesdropper through wireless medium. The closed form expressions and scheme of optimal sensor were derived.

3. EAVESDRP AND SENSORS

In Eavesdrop different data are meant for different sensors, the sensors in the industrial site are used for industrial aspects such as motion of machines, waves generated, pressure generated by the machines, efficiency etc. For the broadcasting of the waves the sensors are used This describes about the phenomenon that consists of a sink node and also contains multiple sensors, and are used in broadcasting of propagation of radio waves, the transmission from the sensor to the sink and from the sensor to the eavesdropper and the difference between these two is the secrecy capacity of the transmission through wireless mode [14]. The main focus of this paper is on the improving the physical layer security by using sensors and the medium is wireless. The transmitted data will be easily intercepted by an eavesdropper if the result or the secrecy capacity will be low or under positive or non negative resulting in the sense due to wireless fading effects as such as obstacles in machinery parts or vibrations through engines.

Cryptographic techniques were used to save or prevent the coded information from eavesdropper having low computing capability but now the information can be decoded easily by the eavesdropper with having high computational capability[14]. The use of distributed sensors in the industry results in the increment of the security purposes in the industry. The vibrations through machinery parts and engines are not good for the propagation of radio waves and causes severe damage to the work of transmission through wireless medium, which results in failure of security and machinery parts which in turn will not work accordingly or properly. By the use of artificial noise, it helps in improving the secrecy capacity and the receiver gets not affected. For the link to be not effected, the number of antennas should be more at the legitimate transmitter then that at the receiver. As artificial noise increase secrecy capacity, but for this it also requires additional power cost. For this purpose, a multiuser scheduling scheme was introduced for Wireless security improvements of the networks, without any power cost.

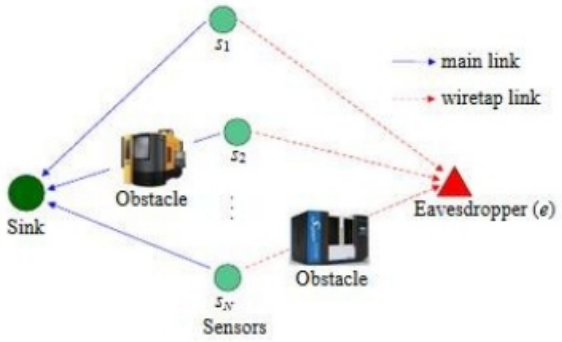

Figure 1. Industrial WSN Setup

Above figure of Industrial WSN in the presence of eavesdropper consists of a sink and N sensors [15]. In this diagram of industrial WSN, it consists of sink; eavesdropper and the lines represent the figure are wiretap link and the main link. N sensors are considered which are represented by S1, S2… Sn. In this N sensors communicate with the sink and eavesdropper intercepts the information passed from sensors to sink and the transmitted medium is wireless transmitted medium. This concept is used in Nakagami model and hence This model is used mainly in literature.

4. SWAPATTACK

For the swap attack, we consider the security reasons for preventing the attack. Directed diffusion and leach is some sensor routing protocols. Security in sensor network is different than traditional network because of computing power. For security purpose encryption techniques are used and also the use of antennas is there. In this paper the topics which are covered or highlighted issues represents the routing should be safe and also represents how to extend the directed diffusion and directed diffusion should be safe. The security should be the main reason for this as to prevent them from the attacks. For routing, good path should be selected so as to reduce energy[16].

The delivery of data should be secure by doing secure Diffusion which reduces traffic in the networking or sending of the data and also provides good quality for the delivery of the data. If the network ability is reduced or transmission of data will be `low then the transmission of message will be suspicious. The main focus of the protocol of routing diffusion is to be the energy efficiency of the network by using hop- to-hop not end-to-end communication protocol.

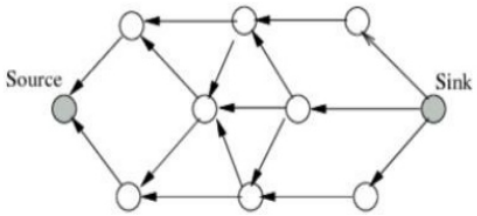

Figure 2. Interest Propagation

Interest is a type of message which describes what the user wants.

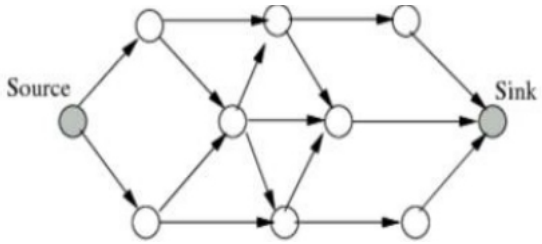

Figure 3A. Initial Gradient Setup

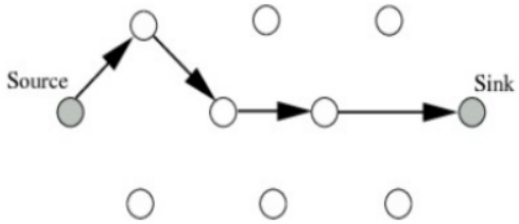

Figure 3B. Send Data & Path Reinforcement

Afore mentioed figures describe about the flow of direction of data and also the data rate and the interest is received from the adjacent nodes . When there will be the activation of the attack then there will be more nodes are included in the route or path and hence this results in the performance of network degradation.

5. CONCLUSION

A Wireless Sensor Network (WSN) sometimes called a Wireless sensor and actuator network) (WSAN). The WSN is build of "nodes" –from few to several hundred or thousand, where each node is connected to one or more sensors. The main application of this are used in industry monitoring and also in military purpose .the focus of this paper is mainly on the betterment of the physical layer security through wireless medium with the help of the sensor scheduling[17]. This is done to increase the security from the eavesdropper. The eavesdropping attack is considered in this paper in which sensors communicate with the sink and eavesdropper intercepts the information passed from sensors to sink and the transmitted medium is wireless transmitted medium and the swap attack was being discovered only the bad routes for routing not the good one path.We can say in swap attack that countermeasure should be used and using the on-off timer, the time gets divides according to different time divisions. By the use of artificial noise, it helps in improving the secrecy capacity and the receiver gets not affected, this results in the increase of Secrecy capacity, without having any effect of the channel capacity.

REFERENCES

[1] W.Shen,T. Zhang, F. Barac, and M.Gidlund,"PriorityMAC: A priority-enhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks,"IEEE Trans. Industrial Informatics, vol.10, no.1, pp. 824-835, Feb.2014.

[2] J.-C. Wang, C.-H. Lin, E. Siahaan, B.-w. Chen and H.-L. Chuang,"Mixed sound event verification on wireless sensor network for home automation,"IEEE Trans. Industrial Informatics, vol.1, no. 1, pp.803-812, feb.2014.

[3] N. Marchenko, T.Andre, G. Brandner,W. Masood, and C.Bettstetter,"An experimental study of selective cooperative relaying in industrial wireless sensor networks,"IEEE Trans. Industrial Informatics, vol. 10,no. 3,pp. 1806-1816,Aug.2014.

[4] T.M. Chi ewe and G.P. Hancke, "A Distributed topology control technique for low interference and energy efficiency in wireless sensor networks," IEEE Trans. Industrial Informatics, vol.8, no. 1,pp. 11-19, Feb. 2012.

[5] Q.Chi, H. Yan,C.Zhang,Z.Pang, and L. Xu,"A reconfigurable smart sensor interface for industrial WSN in IoT environment," IEEE trans. Industrial Informatics, vol. 10, no. 2,pp. 1417- 1425 , May 2014.

[6] F.Gandino, B.Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," IEEE trans. Industrial Informatics, vol. 10, no. 2,pp. 1133- 1143 , May 2014.

[7] M. Cheminod, l. Durante, and A. Valenzano,"Review of security issues in industrial networks," IEEE trans. Industrial Informatics, vol. 9, no. 1,pp. 277-293 , Feb 2013.

[8] Shafiqul Abidin "WSN – An Emerging Technology and its Security Measures" International Journal of Computer Science and Engineering, Vol 5, Issue 9, pp 260-264, September 2018.

[9] S.K. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian wiretap channel," IEEE Trans. Information theory, vol.24, pp.451-456, Jul. 1978.

[10] S. Goel and R.Negi,"Guaranteeing secrecy using artificial noise," IEEE trans. Wireless Communications, vol. 7, no.6, pp. 2180-2189, Jul. 2008.

[11] X. Zhou and M. McKay,"Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," IEEE Trans. Vehicular Technology, vol. 59, no. 8,pp. 3831-3842, Aug. 2010.

[12] D. Goeckel, et al., "Artificial Noise generation from cooperative relays for everlasting secrecy in two- hop wireless networks," IEEE Journal on Selected areas in communications, vol.29, no.10, pp.2067-2076, Oct. 2011.

[13] Y. Zou, X. Wang, and W.Shen, "Physical layer security with multiuser scheduling in cognitive radio networks," IEEE Trans. Communications, vol. 61, no. 12, pp.5103-5113, Dec. 2013.

[14] D. Lee and B.J. Jeong, "Performance analysis of combining space time block coding and scheduling over arbitrary Nakagami fading Channels," IEEE Trans. Wireless communications, vol. 13, no. 5, pp.2540-2551, May 2014.

[15] S.Hussain and X.N. Fernando, "Closed form analysis of relay- based cognitive radio networks over nakagami-m fading channels," IEEE Trans. Vehicular Technology, vol. 63, no. 3,pp. 1193-1203, Mar. 2014.

[16] F.Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," Ad Hoc Networks, vol. 2, no.4 pp. 351-367, Oct. 2004.

[17] Shafiqul Abidin and Mohd Izhar "Attacks on Wireless and its Limitations" International Journal of Computer Science and Engineering, Vol 5, Issue 11, pp 157-160, November 2017.

ISSN Application No. 21726

Security of Internet of Things using Blockchain: An Overview

Amandeep Verma*
*UIET, Panjab University,
Chandigarh, India

ABSTRACT

Now days, Internet of Things (IoT) and Blockchain are new buzzwords across the world. IoT has substantial impact on human life. IoT consists of various heterogeneous devices that are communication over the globe. All IoT applications are producing huge amount of data daily, which raises the concerns about its security. Although there exist centralized access management technologies but there are numerous technical limitations to manage these resources globally. On the other hand, Blockchain, which is based on decentralized and distributed approach, maintains reliable archives of data at different locations with the help of tamper resistant ledger. Blockchain can address the data security concerns in IoT networks. This paper reviews the concepts of IoT, blockchain and advantages of incorporating Blockchain with IoT.

Keywords: Security; Block Chain; IoT

1. INTRODUCTION

Internet of things (IoT) is considered as the prospect or the next generation of internet. IoT connects daily used objects to the internet with a simple goal to provide the users with a smarter and efficient experience in various fields [1]. Numerous IoT applications include healthcare, smart cities, smart grid, water management, smart waste management etc., In the near future, the IoT devices will become an important part of our daily life [2]. Every IoT application uses as well as produces a large amount of electronic data through various sensors to manage heterogeneous resources. This data can be very critical and sensitive. So, its become very important to collect, transfer and process this data in some secure manner, otherwise, it can lead catastrophic events [3]. As, IoT is maturing very fast and making its presence in almost every field of technology, there would not be a single security solution for all IoT applications. Also, with its rapid evolution, it has made itself more prone to cyber-attacks. Therefore, there is an earnestness to mark IoTmore safe [4].

This paper reviews the concepts of IoT, blockchain and advantages and challenges of integrating Blockchain with IoT. Section 2 and section 3 of the paper give the understanding of blockchain technology along with its pillars. Section 4 describes the benefits of integrating IoT with Blockchain. In last, Section 5 concludes the paper.

2. BLOCKCHAIN TECHNOLOGY

Blockchain is one of the emerging technologies in the IT industry. The blockchain technology was first came into existance in 2008 by Satoshi Nakamoto for the cryptocurrency called Bitcoin [5]. Blockchain was the building blocks for this peer to peer electronic cash system, which solved many existing problems in the prior versions of such systems.

The blockchain is a linked list of blocks. Each block consists of records. This list keeps on growing by adding a new block at the end of the record. The adjacent blocks of this chain are secured using cryptography hash functions. The blockchain is inherently resistant to modification of the data inside the blocks. After adding data to one block of the blockchain, it is difficult to modify the contents, as alteration in any data will result in the need for alteration of all the data blocks, which comes after it. Therefore, blockchain is a secured method for storing and transferring the data[6].

Now a day, blockchain technology uses in numerous applications other than Bitcoin. It has the following properties [7]:

a) Decentralized and Distributed: Blockchainis based on decentralized and distributed approach in whichno central authority dictates the rules. Each network node retains areplica of the blockchain information.

b) Data Transparency and Auditability: The data is transparent and auditable as all the peers of blockchain have the full copy ofevery transaction ever executed in the system. So, every transaction is public to all the members.

c) Decentralized Consensus: The transactions over blockchain are validatedby all the nodes of a network instead of by a single entity in centralized approach which leads to decentralized consensus.

d) Secure: The blockchain is tamper-proof and cannot be manipulated by malicious actors.

3. PILLARS OF BLOCKCHAIN

Blockchain technology basically has 4 pillars [8]:

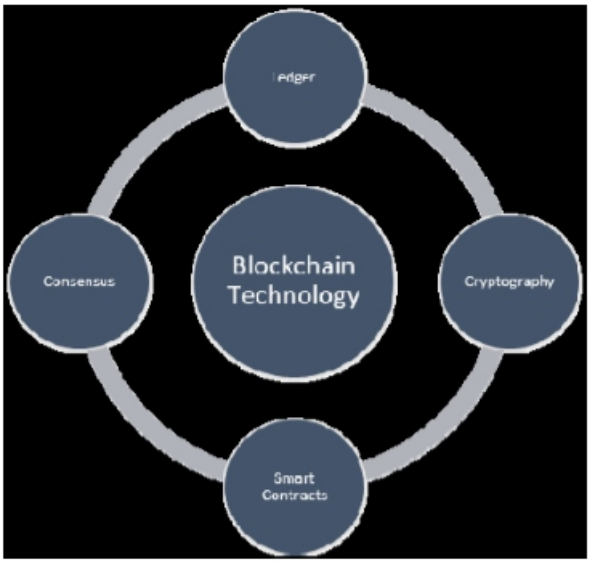

Figure 1. Pillars of Blockchain [8]

a) Consensus, which provides the proof of work (PoW) and verifies the action in the networks

b) Ledger, which provides the complete details of transaction within networks.

c) Cryptography, it makes sure that all data in ledger and networks gets encrypted and only authorized user can decrypt the information.

d) Smart contract, it is used to verify and validate the participants of the network.

4. INTEGRATING IOT WITH BLOCKCHAIN

IoT consists of physical things or objects that are connected through a network of sensors, software's and electronics. It is emerged from the advancements in wireless sensor networks, mobile cloud computing and networking devices [9]. With the rapid development of IoT technology, its applications are also increasing day by day. Healthcare services[10], Smart Water Management, Smart cities [11], Smart home[12], Video surveillance[13], etc. are the major applications of IoT. These applications require large storage and fast computational resources Over the last few years, cloud computing technologies have contributed to providing the IoT with the necessary functionality to analyze and process information and turn it into real-time actions and knowledge. As IoT devices are generally of limited processing and storage capacities, IoT applications can be offloaded to the cloud. Thus, these applications can get the required resources from the cloud and at the same time, users should pay for these resources.

The integration of promising technologies like IoT and cloud computing has proven to be invaluable. Blockchain can improve the IoT by providing a trusted sharing service, where information is reliable and can be distinguishable [14]. In the cases where the IoT information should be securely shared between many participants, this integration would represent a key revolution. As alteration in any data block in blockchain, will result in the need for alteration of all the data blocks, which comes after it. Hence, a data leak in any part of the chain could lead to fraud. Therefore, a blockchain is a secured method for storing and transferring the IoT data.

The advantages of integrating IoT and Blockchain can be, but not limited to [15]

a. Decentralization and scalability: The shift from a present centralized architecture of IoT to a Peer2Peer distributed architecture of blockchain technology, will overcome the problem of failures and bottlenecks of central points. It will also improve the fault tolerance and system scalability.

b. Identity: Using a common blockchain system, all the participants are able to identify every single device. Data provided and fed into the system is immutable and uniquely identifies actual data that was provided by a device. Additionally, blockchain can provide trusted distributed authentication and authorization of devices for IoT applications.

c. Autonomy: With blockchain, devices are capable of interacting with each other without the involvement of any servers. This could benefit IoT applications to provide device-agnostic and decoupled-applications.

d. Reliability: Asblockchain is tamper-proof and cannot be manipulated by malicious actors, data from IoT applications can remain immutable, reliable and distributed over time in blockchain. This will also improve sensor data traceability and accountability.

e. Security: Every data exchange over Blockchainis validated by smart contracts, thus leads to a secure communications between different devices. Current secure standard protocols used in the IoTcan be optimized with the application of blockchain.

5. CONCLUSION

This paper present an overview of the use of Blockchain to resolve the myriad of data security concerns in IoT. We have reviewed the key points where blockchain technology can help improve IoT applications. Advantages of integrating blockchain nodes on IoT devices have also been discussed. It is expected that blockchain will revolutionize the IoT in the coming years.

REFERENCES:

[1] Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-of-Things: Future vision, architecture, challenges and services." IEEE World Forum Internet of Things (WF-IoT), 2014.

[2] Atzori, and Morabito, ―The internet of things: A survey‖, Computer Networks, 54(15), 2787–2805, 2010.

[3] Humayed, Abdulmalik, "Cyber-Physical Systems Security—A Survey." arXiv preprint arXiv:1701.04525, 2017.

[4] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing, J. Netw. Comput. Appl. 67, 99–117, 2016

[5] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2008. Available online: https://bitcoin.org/bitcoin.pdf

[6] C. Li and L.-J. Zhang, ―A blockchain based new secure multi-layer network model for Internet of Things,‖ in Proc. IEEE Int. Congr. InternetThings (ICIOT), pp. 33–41, Jun. 2017.

[7] Xu Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, XinxinNiu, Kangfeng Zheng. "Survey on blockchain for Internet of Things" , Computer Communications, 136, pp; 10-29,2019

[8] Madhusudan Singh, Abhiraj Singh, Shiho Kim. "Blockchain: A game changer for securing IoT data" , IEEE 4th World Forum on Internet of Things (WF-IoT), pp: 52-55, 2018

[9] L. Schubert, K. Jeffery, and B. Neidecker-Lutz, ―The Future of Cloud Computing. Opportunities for European Cloud Computing Beyond 2010,‖ Eur. Comm. Cloud Expert Gr., p. 66, 2010.

[10] D. Gachet, M. De Buenaga, F. Aparicio, and V. Padr??n, ―Integrating internet of things and cloud computing for health services provisioning: The virtual cloud carer project,‖ in 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012, pp. 918–921, 2012

[11] R. Petrolo, V. Loscrí, and N. Mitton, ―Towards a smart city based on cloud of things,‖ in ACM international workshop on Wireless and mobile technologies for smart cities - WiMobCity '14, pp. 61–66 , 2014

[12] S. Y. Chen, C. F. Lai, Y. M. Huang, and Y. L. Jeng, ―Intelligent home-appliance recognition over IoT cloud network,‖ in 9th International Wireless Communications and Mobile Computing Conference, IWCMC 2013, pp. 639–643 , 2013

[13] R. C. Andrea Prati , Roberto Vezzani, Michele Fornaciari, ―Intelligent Video Surveillance as a Service,‖ in Intelligent Multimedia Surveillance, A. C. Pradeep K. Atrey,

Mohan S. Kankanhalli, Ed. Springer Berlin Heidelberg, pp. 1–16, 2013

[14] Oscar Novo. "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT" , IEEE Internet of Things Journal, 5(2), 2018

[15] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz. "On blockchain and its integration with IoT. Challenges and opportunities" , Future Generation Computer Systems, 88, pp: 173-190,2018

ISSN Application No. 21726

Sentiment Analysis on Twitter

[1]Ananth Nath, [2]Anirudh Sudan, [3]Gautam Kumar, [4]Saurabh Bhosale
[1,2,3,4]Department Of Computer Engineering, MIT Academy Of Engineering, Alandi(D), Pune.
E-mail: [1]ananthnath.14@gmail.com

ABSTRACT

Twitter is a well-known micro-blogging website which allows millions of users to share their views and opinions on various matters. These tweets are displayed on the twitter UI and various users can interact with each other by using the @redirection to include another username. The trending topics are displayed on the UI. A trending topic is one which is currently the most popular. In this day and age where nearly a billion people have access to the internet to express their views on their day to day activities, data mining and analyzing data from social networks can be difficult because of the large amounts of data involved. Sentiment analysis, which is also called opinion mining is the field of study which analyzes peoples opinions, sentiments, evaluations, appraisals, attributes and emotions towards entities such as products services, organizations, individuals, issues, events, topics, and their attributes through twitter. Sentiment analysis on a website like twitter can play a vital role in helping advertisers and market strategists. A sentiment analysis machine is a type of AI which receives the tweets as its input and after evaluating the input, it will display the sentiment of the user. If implemented properly sentiment analysis can be useful in predicting trends in the market as it provides an insight into the minds of users and potential customers.

Index Terms—Sentiment, Analysis, Trending, Data Mining, Ar-tificial Intelligence.

I. INTRODUCTION

Big corporations are turning to the media websites like Facebook and twitter to get closer to their customers. Not only do these platforms help the big companies advertise their products or information, they even provide a broad vision of what goes inside the minds of an average person and this is where sentiment analysis comes into play. The analysis of what the consumers feel about the products be it commodities, new music albums or movies, gives the companies an idea of how to make their brand more desirable to the masses. In this project we explain how sentiment analysis can be carried out on twitter which is a micro-blogging website that handles millions of tweets (updates by users) every day. The average sentiment regarding a product is categorized to positive, negative or neutral. Recent studies have shown that humans are able to correctly estimate the sentiment of a sentence/speech or conversation accurately only 80 percent of the time. So the machines that were previously designed and had success rate of 30-40 percent are considered a success. Recently efforts have been made to make these machines more efficient by using advanced NLP.

II.SENTIMENT ANALYSIS

It is the process of computationally identifying and catego-rizing opinions expressed in a piece of text, in order to deter-mine the writers attitude towards a particular topic or product. It has been widely used to extract the opinions or views of people on various topics, products or persons. Opinion Mining or Sentiment analysis is conducted by groups or organizations to predict the views of people about certain persons, products or other topics of interest. It has been used to analyze the mood of the public to rate movies, contestants (political campaigns, reality shows), music and other topics or products and thus, is used in formulating estimates. Some firms use twitter data to analyze the tweets and generate the general opinion on their product. Semantic analysis is employed on the contextual contents of each tweet and predicts response of selected group of people. With digital marketing being employed these days for advertising on social media websites every day, sentiment analysis comes in handy. Big firms collect millions of tweets about their product and analyze them using sentiment analysis tools and determine the performance of their product in the market. They use emoticons and hashtags to find the tweets pertaining to their products. For example- suppose a firm A has its twitter page and uses it to advertise their products on the internet. The firm A has a million followers on its page and they tweet about their products and schemes every day. It is nearly impossible for their advertising team to read through each tweet and determine the average opinion of that product. For this they use a model that fetches tweets about that products and collects them temporarily. Now it compares the polarity of the emoticons and the keywords with the adjectives and defining words in a predefined database. After analyzing all the tweets, the model is able to determine whether the average is positive, negative or neutral.

A. BACKGROUND

III. LITERATURE SURVEY

1. Correlation Analysis of User Influence and Sentiment on Twitter Data- Uses reciprocity to calculate and do the analysis. Calculates value of influence using Bayes theory, using number of retweets.
2. Crime Prediction Using Twitter Sentiment and Weather-We can predict response or display average response to an entity. Paid attention to emoticons.
3. Visual Sentiment Analysis on Twitter Data Streams Sentiment analysis is classified into:

   I. Topic-based.

   II. Stream analysis.

   III. Visual analysis.

Pixel sentiment analysis that comes under visual analysis focuses on geo-maps to show the sentiments.

4. Twitter Sentiment Analysis Used lexicon- based and ma-chine learning approach for sentiment analysis. Output was stored in JSON file and the data was represented using a pie-chart.
5. SASM: A Tool for Sentiment Analysis on Twitter- Analyzes the data from twitter and describes the process to emoticon sentiment analysis resource. Uses lexicon based approach using fuzzy linguistic logic hedges for analysis.
6. Sentiment Analysis on Tweets for Social Events TSAM model had three modules:
   I. Sentiment identification.
   II. Sentiment aggregation.
   III. Scoring module.
7. Twitter for Sentiment Analysis: When Language Re-sources Are Not Available- Lexicons contain lists of words an-notated with their emotional assessments. Annotated word lists are one of the tools frequently used in sentiment analysis to detect a mood or classify emotions within a text. Constructed a method that makes it easier for translation of languages other than English.
8. Sentiment Analysis and Summarization of Twitter Data-Could be utilized to generate extractive summaries of a col-lection of multi documents.

IV. PROPOSED SYSTEM

The Tweets are usually analysed because they tend to have the potential to map the trend amongst the people. These tweets carry the sentiment of people related to a specific topic not only in the form of words that they use but also is expressed with the help of emoticons.

Use of this known fact while working on an analysis tool can help us to increase its overall efficiency since emoticons may carry a polarity that is either positive, negative or neutral.

Figure 1 shows the work flow of the proposed system. Twitter API is used to search query for tweets. The tweets are then processed according to the model.

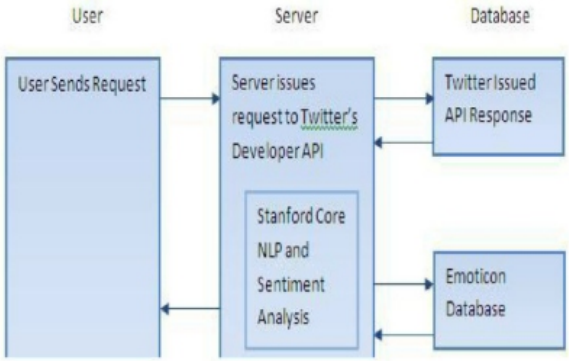

Fig 1:Architecture

The above figure depicts the basic structure of the sentiment analysis tool. The user via the sentiment analysis tool requests the Twitter API to allow access to tweets via the usage of OAUTH standard. Once the access to tweets is authorised, the tweets are run through the Stanford NLP tool for preprocessing i.e. removal of non-English tweets and breaking down of tweets into individual words. These words are run through the database for matching.

The basic workflow architecture is as follows:

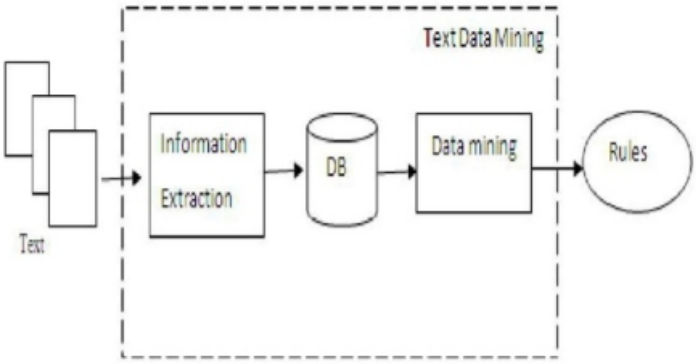

Fig 2: Workflow

V. DETAILED DESIGN

The approach to sentiment summarization consists of four main steps:

1. Finding the target item features that people have tweeted for item.
2. The tweets are retrieved and to kenized.
3. These tokens are analyzed and then compared with the database or the annotations list containing positive words and the database the annotations list containing negative words.
4. The positive sentiment and negative sentiment is calcu-lated.
5. If the calculated positive sentiment is more than the negative calculated sentiments, then the overall sentiment is positive.
6. If the calculated positive sentiment is less than the negative calculated sentiments, then the overall sentiment is negative.
7. Otherwise it is considered neutral.

The System flow is depicted in the following image.

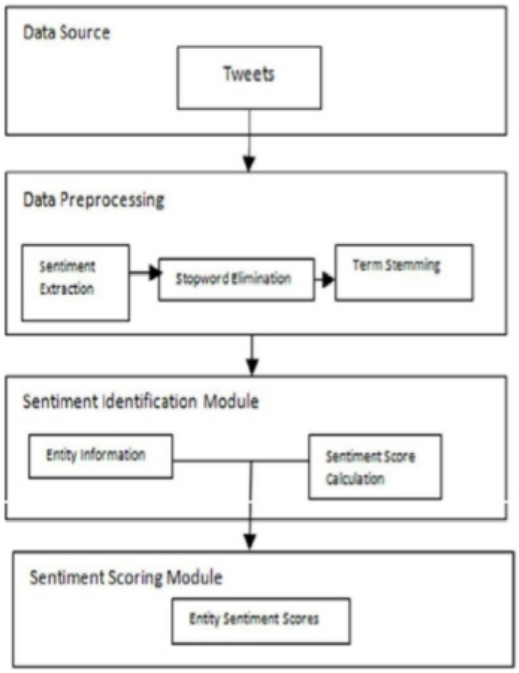

Fig 3: System Flow

The following Use cases show the workflow of the proposed analysis tool:

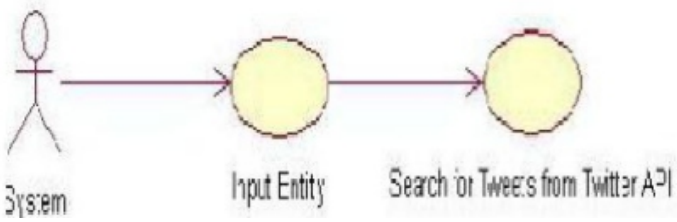

Fig 4: Use case for Tweets Search

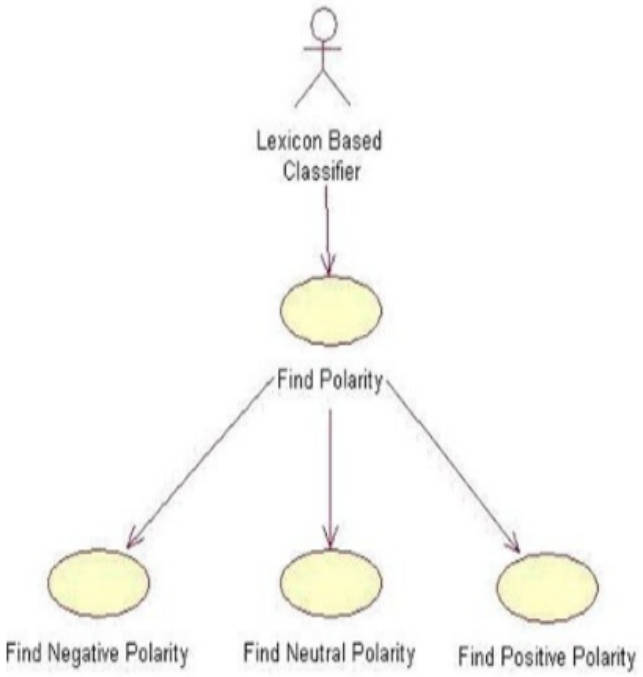

Fig 5: Use Case for polarity

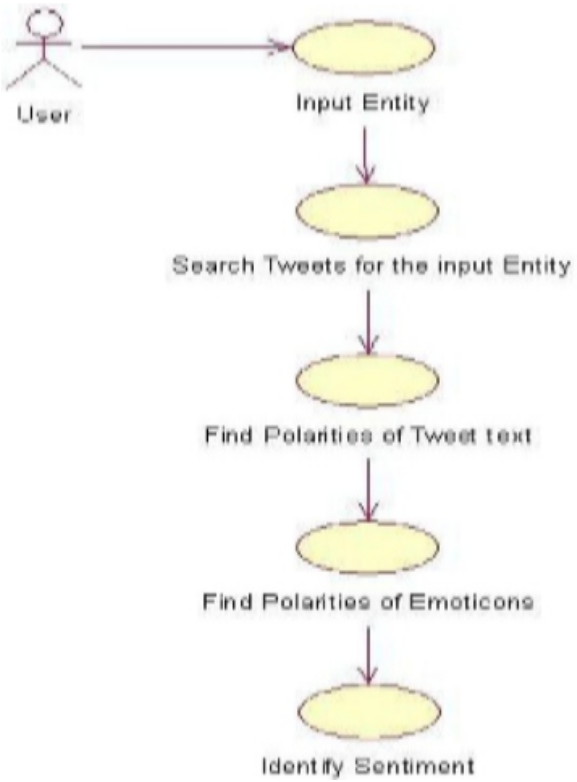

Fig 5: Use Case for sentiment analysis

CONCLUSION

We would like to conclude by saying that sentiment anal-ysis is increasingly becoming one of the popular tools for businesses and entities that wish to determine the opinions and responses of the public to their products or their individ-ual selves. Sentiment analysis has been used in the past to aid election campaigns, advertisements. We can use the twitter database to access the tweets of our specified area and then systematically process these tweets to obtain their sentiment as described above.

FUTURE WORK

Sentiment analysis is a field that has tremendous scope for improvement. Some of the areas which can be improved are as follows:

Language translation: The current sentiment analysis tools have been designed for only one language at a time.Most commonly English. With Language Translation many more languages can be considered as these tweets will not be discarded

Include abbreviations: Currently there is a huge differ- ence between the English we speak and our written English. People tend to use a number of short forms or abbreviations such as LOL, ASAP, etc. Some abbreviations have been around for a whle and have been incorporated into our dictionary but the sentiment analysis tool can't keep up with each new abbreviation.

Have a higher accuracy rate: A sentiment analysis tool must be as accurate as can be.A higher accuracy rate will be more feasible in the future due to designs of more extensive AI.

ACKNOWLEDGMENT

The authors would like to thank Mrs. Mayura Kulkarni for her efforts and her guidance. We would like to thank her for allowing us access to IEEE publications and for her inputs.

REFERENCES

[1] Fadhli Mubarak bin Naina Hanif, G. A. Putri Saptawati, "CORRE-LATION ANALYSIS OF USER INFLUENCE AND SENTIMENT ON TWITTER DATA".
[2] Xinyu Chen, Youngwoon Cho, and Suk young Jang, "Crime Prediction Using Twitter Sentiment and Weather".
[3] Ming Hao, Christian Rohrdantz, Halldr Janetzko, Umeshwar Dayal Daniel A. Keim,Lars-Erik Haug, Mei-Chun Hsu, "Visual Sentiment Analysis on Twitter Data Streams".
[4] Onifade O.F.W, Malik M.A., "SASM: A Tool for Sentiment Analysis on Twitter".
[5] Aliza Sarlan, Chayanit Nadam, Shuib Basri, "Twitter Sentiment Analysis".
[6] Seyed-Ali Bahrainian, Andreas Dengel, "Sentiment Analysis and Summarization of Twitter Data".
[7] Meral, Banu Diri, "Sentiment Analysis on Twitter".
[8] Alexander Pak, Patrick Paroubek, "Twitter for Sentiment Analysis: When Language Resources Are Not Available".
[9] Xujuan Zhou,Xiaohui Tao, Jianming Yong, "Sentiment Analysis on Tweets for Social Events".

ISSN Application No. 21726

Spam Proof Tagging System using Trust Modeling Algorithm

[1] Seema Bhuravane, [2] Dipti Patil
[1,2]Computer Engineering Department PIIT New Panvel, Mumbai University, India
E-mail: [1]skbhuravane@gmail.com, [2]dypatil75@gmail.com

A B S T R A C T

Tagging in online social networking site is very popular these days, as it facilitates search and retrieval of various resources such as text, images, videos, etc. Despite the advances in social networking over the past few decades, one of the important challenges that user continuously facing is spam. Noisy and spam annotations often make it difficult to perform an efficient search. The shared content is sometimes assigned with inappropriate tags for several reasons. Users may make mistakes while tagging and irrelevant tags and content may be maliciously added for their advertisement or self- promotion. Consequently, assigning tags to resources has a risk that wrong or irrelevant tags eventually prevent users from the benefits of annotated content. One important challenge in tagging is to identify the legitimate tags for given content, and at the same time, to eliminate spam tags. Trust can predict the future behavior of users to avoid undesirable influences of untrust-worthy users. Here we proposed a trust-worthy system that has been designed with the objective to minimize spam tagging and posting in social networking sites with the adaptation of classification algorithms.

Keywords— Tagging, Tagging system, Trust modeling, Tag spam.

I. INTRODUCTION

Social networking sites make it possible to users to form social relations among people who share similar interests, real life activities or connections. Whenever information is exchanged on the Internet, spammers are everywhere and they try to take advantage of the information exchange structure for their own benefit, while troubling and spamming others. Before social tagging became popular, spam content was observed in various domains. First in e-mail, and then in Web search networks have been also influenced by malicious peers, and thus various solutions based on trust and reputation have been proposed, which dealt with collecting information on peer behavior, scoring and ranking peers, and responding based on the scores.

Social tagging became popular with the launch of various sites like Delicious and Flickr. After that, different social tagging systems have been built to support tagging of a variety of resources like text, images. For given a particular resource, tagging is a process where a user assigns a tag to an object. Most tagging systems such as Delicious and Flickr are collaborative in nature in that they allow users to share and peruse tags and resources from other members of the community. On Delicious, a user can

assign tags to a particular bookmarked URL. On Flickr, users can tag photos uploaded by them or by others. Whereas Delicious allows each user to have her personal set of tags per URL, Flickr has a single set of tags for any photo. On blogging sites like Blogger, Wordpress, Livejournal, blog authors can add tags to their posts. On micro-blogging sites like Twitter, hash tags are used within the tweet text itself. On social networking sites like Facebook users often annotate parts of the photos. Users can also provide tagging information in other forms like marking something as "Like" on Facebook. Upcoming event sites can allow users to comment on and tag events. Despite the advances in social networking sites over the past few decades, one of the important challenges that user continuously facing is spam. Malicious users continue to innovate ways to take advantage of public trust. Literature survey shows that the spam on Facebook and YouTube websites are extremely higher than what may be noticed on other social media websites.

Tagging services in social networks, e.g., Flickr, Delicious, YouTube, have grown in significance on the Internet based on the number of participating users. In a typical tagging system, each specific resource like post, photo, URL is annotated with some tags. Resource annotators are the users, who have annotated a specific resource with some tags and the relation <tag, resource> that annotates a resource with a tag is called an annotation. Annotation preserves the association between the tag and resource. When the user issues a tag in search bar, the system retrieves resources associated with this tag. Then, the user may collect some of the resources, and annotates it with some tags. By literature survey many recent studies indicated that the tagging systems are vulnerable to tag spam and malicious users generate the incorrect or misleading tags to confuse the normal participants in the system. For instance, some attackers may repeatedly annotate some images in Flickr with the incorrect tags; so that the normal users, without sufficient knowledge about other participants, may be mislead to open an undesirable image.

1.1 Trust Modeling

Proposed social tagging system makes use of trust modeling algorithms for classification of spam and legitimate texts. Authors in paper [6] proposed that spam or noise can be injected at three different levels: spam content, spam tag-content association, and spammer. Trust modeling can be performed at each level separately or different levels can be considered jointly to produce trust models. For example, to assess a user's reliability, one can consider not only the user profile, but also the content that the user uploaded to a social system. We categorize trust modeling approaches into two classes according to the target of trust, i.e. user trust modeling and content trust modeling. Content trust modeling is used to classify content like posts, images, and web pages as spam or legitimate. In this category, the target of trust is content, and thus a trust value is given to each content based on its content and/or associated tags. User trust modeling is of two types: static and dynamic.

1.2 Problem Statement

Tagging systems are known to be vulnerable to tag spam. These systems depend on user-generated content, making them both extremely dynamic and tempting targets for spam. So the increasing interest in tagging systems also increases danger from spam. Sometimes the shared content is assigned with inappropriate tags for several reasons. Users are human beings and may commit mistakes but it happens rarely. Most of the time, spammers provide wrong tags on purpose for their advertisement, self-promotion, or to increase the rank of a particular tag in search engines. If this kind of spam is left unchecked, could harm the system in many ways, such as resource sharing openness, information retrieval effectiveness and user experience, etc. One of the major issues in tagging is to identify the most appropriate tags for given content, and at the same time, to eliminate noisy or spam tags. Thus, spam-fighting mechanisms need to be developed to combat the flexible strategies of spammers.

Here we try to understand the problem better, to examine to what extent tagging systems can be manipulated by spammers and to try to devise schemes that may fight spam.

1.3 Review Of Literature

We studied the concepts of using machine learning techniques and classifiers which are used for email spam filtering. As there are various issues related to social tagging systems, we applied all these techniques to build the proposed system which specifically try to combat spam in social tagging systems and try for very efficient results.

This article [1] surveys three categories of potential countermeasures those based on detection, demotion, and prevention. Detection-based strategies attempt to identify spam and remove it or reduce its prominence. Demotion-based strategies attempt to lower the ranking of spam in ordered lists. Prevention based strategies attempt to make contribution of spam more difficult by changing interfaces or limiting user action.

In this paper [2] proposed system uses TrustRank for Combating Web spam. Search engines are today combating web spam with a variety of ad hoc, often proprietary techniques. This paper introducing a comprehensive solution to assist in the detection of web spam. Experimental results show that we can effectively identify a significant number of strongly reputable (non-spam) pages. This paper [3] defines an ideal tagging system that combines legitimate and malicious tags. This model allows studying a range of user tagging behaviors, including the level of moderation and the extent of spam tags, and comparing different query answering and spam protection schemes.

In paper [4] authors proposes the Social Trust framework for tamper resilient trust establishment in online communities. Social-Trust provides community users with dynamic trust values. Authors experimentally evaluate the Social-Trust framework using real online social networking data consisting of millions of My Space profiles and relationships.

In this paper [5], authors introduce a set of initial features that can be used for spam classification. These features are evaluated with well-known classifiers (SVM, Naive Bayes, J48 and logistic regression) against a simple baseline of representing a user by the usage of tags.

This paper [6] surveys recent advances in techniques for combating such noise and spam in social tagging. Author proposed a model of a social tagging system that consists of users, contents and tags. Also classified existing studies in the literature into two categories, i.e., content and user trust modeling. Representative techniques in each category were analyzed and compared.

In this paper [7], authors make a contribution towards the development of a privacy-preserving collaborative tagging service, by showing how a specific privacy-enhancing technology, namely tag suppression, can be used to protect end-user privacy. For removing spam author uses Naive Bayes classifiers which is most successful known algorithms for learning to classify text documents.

In this paper [8], the system that classified spam mail and other mail (regular mail) was constructed by two filters with Bayesian theory and SVM(Support Vector Machine) used well by the text classification task as a text classification algorithm. In this paper [9] authors construct different filters using three types of classification, including Naïve Bayes, SVM, and KNN.Naïve Bayes spam email filters are a well- known and powerful type of filters. In this paper [10], authors surveyed social tagging with respect to different aspects. They discussed different user motivations and different ways of tagging web objects. They presented a summary of the various tag generation models. In paper [11] Authors examines the effectiveness of statistically-based approaches

Naive Bayesian anti-spam filters, as it is content- based and self-learning (adaptive) in nature.

II. PROPOSED SYSTEM

2.1. System Framework

The proposed system has been designed with an objective to minimize spam tagging and posting in social networking scenario. The two views for the system would be: admin and user.

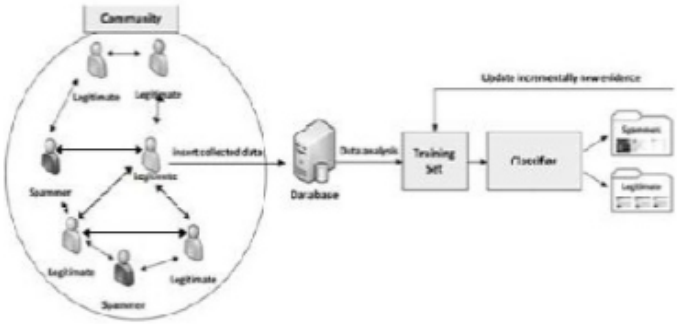

Figure 1: System framework

An admin is a person with complete access to the system. The admin panel would be facilitated with vital features to regulate the postings made by the user. Likewise, a reporting feature would assist him to analyze the spam users in the system.

Admin view would have the right to define the stop words and base words in the application. A stop word can be defined as a word which doesn't affect the logic of the statement and is present in the sentence for grammatical fulfillment eg. a, the, is, that etc. On the other hand, a base word can be defined as a word which directly impacts the logic of the statement e.g. reach, jump, travel, drive etc. Stemming describes the process of transforming a word into its root form.

A user will have the feature to register itself independently on the website by providing essential details suggested by the application. A user can log into the system by facilitating essential login credentials in the application. A user would have a feature to add other users as friends in the system.

A user can add new posts in the application which gets linked to his profile. The system checks for spam (Content Analysis) based on the tags selected by the user for making the post. Depending upon the relation and relevancy of the used tags and the content, the system approves it. Likewise, the system also checks the user trust - static based on the history of posts that he had made in the system. It helps the system to comprehend the nature of the user and its subsequent classification. Also, it considers the posts made by the friends of the users. These factors help to assign a weight of trust to the users' profile and his posts.

Based on all the three checks above, the system fathoms whether the post is a spam or not. The decision is automated and system uses the base words and stop words defined by the admin in his login. A user is permitted to make only limited posts. Once he crosses the threshold, the system blocks the user. A user also has the feature to search for posts made by other users and vote up or vote down to them.

An admin sees a list if users which are blocked over a period of time and also checks the results generated by the system Bayesian spam filtering algorithm. It makes use of a naive Bayes classifier on bag of words features to identify spam tag, an approach commonly used in text classification. Naive Bayes classifiers work by correlating the use of tokens (typically words, or sometimes other things), with spam and non-spam tags and then using Bayesian inference to calculate a probability that a tag is or is not spam.

Our system that classified spam tags and regular was constructed by two filters with Bayesian theory and KNN used well by the text classification task as a trust modeling algorithm. Trust modeling algorithms takes known set of input data and known responses to the data as output, and trains a model to generate reasonable predictions for the response to new data. System framework is described to demonstrate how a social tagging system can benefit from trust modeling with the adaptation of classification algorithms.

The proposed system framework requires training of keywords that can be provided by a previous set of spam and legitimate messages. It keeps track of each word that occurs only in spam, only in legitimate messages, and in both. Based on these word occurrence statistics also called tokens, incoming unseen messages are processed and classified accordingly.

2.2. System Model

System model is described to demonstrate how a social tagging system can benefit from trust modeling with the adaptation of classification algorithms. System model consists of following steps:

- **Steps:**

1. Training data of annotated tags

- In training data set I want to introduce some tag examples to demonstrate process of Navie Bayes classification.

2. A set of classes

- In our case two possible classes
- Can further be personalized

3. Feature Extraction

- Tokenization

- Domain specific features
- Most often features to be selected

4. Classify (each message)

- Calculate posterior probabilities

5. Evaluate results

2.2.1. Spam Filtering Method:

i. Naive Bayes classifiers

Naive Bayes classifier is one of the most successful known algorithms for learning to classify text documents. Bayesian spam filtering has become a popular approach to distinguish spam texts from legitimate texts. The filter doesn't know probability of new word in advance, and must first be trained so it can build them up. Naive Bayes classifiers are a family of simple probabilistic classifiers based on applying Bayes' theorem with strong (naive) independence assumptions between the features. To train the filter, the user must manually indicate whether a new tag is spam or not. For all words in each training posts, the filter will adjust the probabilities that each word will appear in spam or legitimate keywords in its database. The naive Bayes classifier's beauty is in its simplicity, computational efficiency, and good classification performance.

Let Pr(S) be the probability that a message is spam which is the total number of spam messages divided by the total amount of messages. Now the goal would to be taking a feature of word that describes a spam message and calculate the probability of that.

$$P_r(S|W) = \frac{Pr(W|S) \cdot Pr(S)}{Pr(W|S) \cdot Pr(S) + Pr(W|H) \cdot Pr(S)}$$

Here Pr(S|W) is the probability that a message is a spam, knowing that the word is in it;Pr(S) is the overall probability that any given message is spam; Pr(W|S) is the probability that the word appears in spam messages;Pr(H) is the overall probability that any given message is not spam (is "ham"); Pr(W|S) is the probability that the word appears in ham messages [21].

For evaluating result consider the message m and determine the value for feature w. Then take the calculated probabilities and calculated the probability that it is spam and the probability that it is legit. Compare those two probabilities to classify the message as spam or legit.

ii. KNN classifier

K nearest neighbors is a simple algorithm that stores all available cases and classifies new cases based on a similarity measure (e.g., distance functions). One advantage of this algorithm is that there isn't really a training phase. However, for classification of a message, all distances between that message and all the training examples must be calculated and the knearest neighbors need to be found and counted.

- **Algorithm**

Assumption: there are previously minimum 10 post detected.

1. define k=5,
2. Identify parameter for input post.
3. Compare with all spam post.
4. Calculate distance of current post with other spam post using formula:-
5. x=avg(total count for all keywords for that post)
6. y=avg(support value)
7. d= sqrt((x1-x2)^2 + (y1-y2)^2 + (z1-z2)^2….)
8. Store d in array, with post id.
9. end for loop.
10. sort distance array
11. Identify top k value.
12. Calculate avg between these 5 distance value.
13. this is k distance for spam.
14. repeat above step for valid post.
15. identify k distance which is less.
16. return less=spam

For evaluating result consider a message m, find the k nearest neighbors and count the number of each label whether spam or not that are given from the neighbors. If there are more spam messages in the k nearest neighbors then it is classified as spam. If not, then that message is classified as legitimate tag.

III. RESULT ANALYSIS

System shows classification of spam (bad) posts from total posts for both the algorithms on dashboard as shown in figure 3.Then figure 4 shows classification of tags separately for each users using KNN classifier.

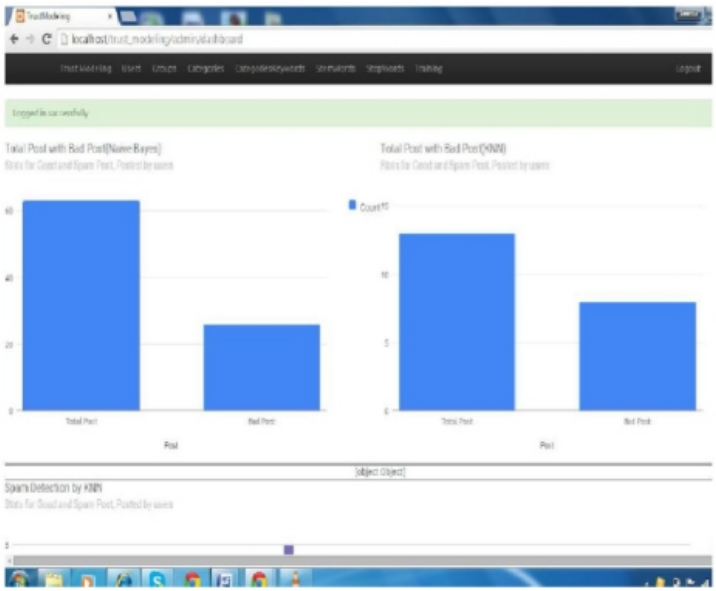

Figure 2: Classified posts for both algorithms

Figure 3: Classified posts using KNN algorithm

CONCLUSIONS

Here we dealt with one of the key issues in social tagging systems: combating noise and spam. Based on categorization of trust modeling i.e content and user, we focused on classification of contents of social tagging system as spam or legitimate. In a social tagging system, spam or noise can be injected at three different levels: spam content, spam tag- content association, and spammer. Trust modeling can be performed at each level separately or different levels can be considered jointly to produce trust models. Trust Modeling is one of the current techniques for noise and spam reduction focus only on textual tag processing and user profile analysis. Proposed model is described to demonstrate how a social tagging system can benefit from trust modeling with the adaptation of classification algorithms.

The proposed system has been designed with an objective to minimize spam tagging and posting in social networking scenario. The system checks for spam (Content Analysis) based on the tags selected by the user for making the post, history of posts and user profile. Here we use Naive Bayesian Model for developing proposed system to filter spam tags in social tagging systems. Then we use KNN classifier for spam filtering and check the result. Comparative study states that KNN gives better result than NB classifier.

ACKNOWLEDGMENTS

We would like to thank Prof. Dipti Patil for helpful discussions. We would also like to thank the anonymous reviewers for their helpful suggestions.

REFERENCES

[1] P. Heymann, G. Koutrika, and H. Garcia-Molina, "Fighting spam on social Web sites: A survey of approaches and future challenges," IEEE Internet Comput., vol.11, no. 6, pp. 36–45, Nov. 2007.
[2] Z. Gyongyi, H. Garc ia-Molina, and J. Pedersen, "Combating Web spam with TrustRank," in Proc. VLDB, Aug. 2004, pp. 576–587.
[3] G. Koutrika, F. A. Effendi, Z. Gyöngyi, P. Heymann, and H. Garcia-Molina, "Combating spam in tagging systems: An evaluation," ACM TWEB, vol. 2, no. 4, pp.22:1–22:34, Oct. 2008.
[4] J. Caverlee, L. Liu, and S. Webb, "SocialTrust: Tamperresilient trust establishment in online communities," in Proc. ACM JCDL, June 2008, pp.104–114.
[5] B. Krause, C . Schmitz, A. Hotho, and G. Stum, "The antisocial tagger: Detecting spam in social bookmarking systems," in Proc. ACM AIRWeb, Apr. 2008,pp. 61– 68.
[6] I.Ivanov, P. Vajda, J. S. Lee, and T. Ebrahimi, "In tags we trust: Trust modeling in social tagging of multimedia content," IEEE Signal Proc. Mag., vol. 29, no. 2, pp. 98–107, Mar. 2012.
[7] L.Sundarrajan, S.Gunasekaran "Social Networks Privacy-Preserving On Collaborative Tagging and Spam Filter Using Naive Bayes Algorithm" IJIRCCE, Vol. 2, Issue 10, October 2014.
[8] Ayahiko Niimi, Hirofumi Inomata, Masaki Miyamoto and Osamu Konishi "Evaluation of Bayesian Spam Filter and SVM Spam Filter"2004.
[9] Yun-Nung Chen, Che-An Lu, Chao-Yu Huang "Anti- Spam Filter Based on Naïve Bayes,SVM, and KNN model",AI TERMPROJECT,2009.
[10] Manish Gupta, Rui Li, Zhijun Yin, Jiawei Han "An overview of social tagging and Applications",Springer International Publishing, Mar. 2011.
[11] Vikas P. Deshpande, Robert F. Erbacher, and Chris Harris "An Evaluation of Naïve Bayesian Anti-Spam Filtering Techniques", IEEE, June 2007.
[12] Flickr Web site.[Online]. Available:http://www.flickr.com
[13] Facebook Web site. [Online] .Available: http://www.facebook.com
[14] Delicious Web site. [Online]. Available: http://www.delicious.com
[15] eBay Web site. [Online]. Available: http://www.ebay.com
[16] Amazon Web site. [Online]. Available: http://www.amazon.com
[17] Epinions Web site. [Online]. Available: http://www.epinions.com
[18] Twitter Web site. [Online]. Available: http://www.twitter.com
[19] Panoramio Web site. [Online]. Available: http://www.panoramio.com
[20] MySpace Web site. [Online]. Available: http://www.myspace.com
[21] http://en.wikipedia.org/wiki/Bayesian_spam_filtering
[22] http://techcrunchies.com/growth-of-social-media- spamstatistics-for-2013
[23] Paul Graham: A Plan for Spam, http://www.paulgraham.com/spam.html
[24] https://en.wikipedia.org/wiki/K- nearest_neighbors_algorithm
[25] YouTube Web site. [Online]. Available: http://www.youtube.com

ISSN Application No. 21726

Internet of Things based System for Remote Monitoring of Weather Parameters and Applications

[1] Prachi H. Kulkarni, [2] Pratik D. Kute
[1,2]Department of Electronics and Telecommunication Engineering College of Engineering, Pune
E-mail: [1]prachi71192@gmail.com, [2]pk11235@gmail.com

A B S T R A C T

With the development in microcontroller technology, internet accessibility, cloud computing and miniaturization of electronic components, it has now become possible to connect physical objects to the Internet making the World Wide Web an 'Internet of Things (IoT)'. Smart environments created using Internet of Things can provide energy efficient solutions to day-to-day challenges. The paper has discussed the proof of concept for an IoT device that collects data regarding physical parameters, using a sophisticated microcontroller platform, from various types of sensors, through different modes of communication and then uploads the data to the Internet. The presented device has been designed for remote monitoring of weather parameters. The paper focusses on the technique of uploading acquired data online, so that the device can be used to remotely monitor weather parameters and eventually analyze climate change patterns. The paper also discusses the basic concept of Internet of Things and its potential applications, especially for environment monitoring.

Keywords- Internet of Things, Remote Weather Monitoring, IoT Applications, Environment Monitoring, Arduino, Twitter, Sensors

I. INTRODUCTION

Internet of Things (IoT) has the potential to make the world more hospitable for present and future generations of humanity. IoT devices can be deployed in numerous ways for sustainable development. An IoT [1] device can be used to measure physical parameters pertaining to a physical object and upload them real-time to an online repository i.e. to a cloud storage where they can even be analysed in real-time. Thus, the measured data can be observed from anywhere around the world using Internet-enabled devices. IoT, integrated with cloud computing, allows for decentralization of data storage, processing and analysis. The collected data can also be used to automatically control other remote devices, using machine-to-machine (M2M) communication through the Internet.

As a result of these features, an IoT device enables remote monitoring of the environment without the need to visit the site frequently. This can make monitoring possible even in difficult geographical terrains. It can also reduce the manpower requirement and thus the risk involved in visiting inhospitable sites. Further, it can reduce the consumption of fuel and energy required to visit the site, thereby reducing pollution and carbon footprint. IoT can also provide automated energy efficient solutions to everyday applications.

The fundamental components [1] of an IoT device are: Control Unit, Power Supply, Input Devices, Output Devices, Internet Mechanism etc. An IoT device can efficiently connect physical objects placed at a great distance from each other without the need of direct physical connection. Thus, IoT devices have significant applications in almost all fields. Some of them are as follows:

1. Healthcare

Implantable as well as wearable wireless devices can be used to monitor critical parameters of a patient's body in real-time, thus improving the efficiency and effectiveness of healthcare solutions, especially during emergencies.

2. Automotive Applications

Parameters such as engine temperature, tyre pressure, hydraulics, speed, fuel level etc. can be monitored in real-time to determine necessary safety measures.

3. Manufacturing Sector

Monitoring every step in a product life cycle can help to take essential steps for attaining higher accuracy and precision in the manufacturing process.

4. Energy Efficient Solutions

Various devices such as air conditioners, heaters, garden sprinklers in homes, offices etc. can be switched on remotely only if the sensors indicate a need for the same, thus helping to conserve energy.

5. Smart Metering for Smart Cities

Smart metering involves establishing communication between various meters of regular use (for example, gas or electricity meters) and a central station. This makes the data storage and billing centralized and thus increases the reliability and accuracy of the billing process. Enhanced services made available through smart metering can also help the consumer to monitor and manage the usage of the resources. Smart metering systems coupled with energy efficient solutions, for usage of civic resources, can contribute significantly to the development of smart cities.

6. Environmental Monitoring and Management Integrated Information Systems [2] can be developed that combine technologies like Internet of Things, Cloud Computing, Remote Sensing, Geographical Information System, Global Positioning System etc. for monitoring the environment and analysing climate patterns and changes in them.

II.OVERVIEW

The presented design is a proof of concept for a standalone IoT device covering different types of sensors viz. binary switch sensor, analog sensor and digital bit-stream sensor along with both wired and wireless modes of communication to the control unit. All these types of sensors and modes of communication are demonstrated for IoT, through a remote weather monitoring system which measures the following weather parameters:

1. Daylight: Using a photodiode as a wired binary switch sensor
2. Humidity: Using a wired analog humidity sensor
3. Temperature: Using a digital bit-stream temperature sensor via wireless medium employing wireless RF modules.

The daylight parameter is used as an input to control lamp(s) which switches on when it is dark and switches off when there is light. Using an Ethernet connection, the weather parameters are uploaded to a Twitter [3] account which automatically time-stamps the data. The block diagram of the device is shown in Fig. 1. The types of sensors and modes of communication can be changed according to requirements of specific applications.

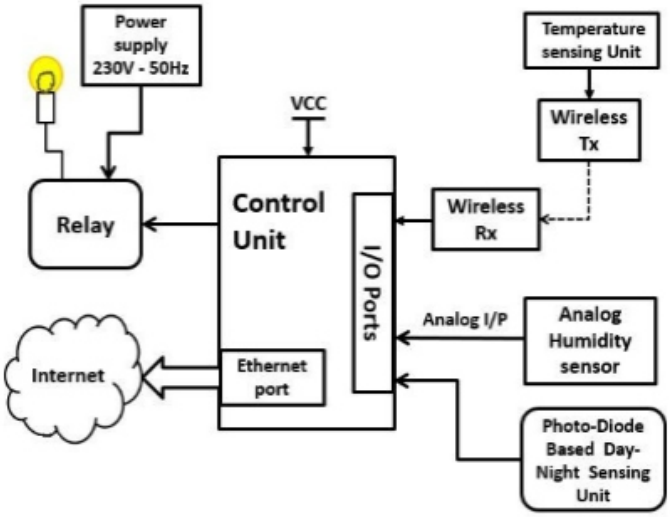

Fig. 1. IoT Device for Weather Monitoring System

The presented design is based on the Arduino Uno R3 (Arduino) [4] platform which is appropriate for the simple application under consideration, unlike more advanced platforms like Raspberry Pi [5]. Unlike the processor-based Raspberry Pi [6], the Arduino is a micro-controller based platform. As a result, it can be

more application specific, making optimal usage of memory and I/O resources and thus reducing its cost. The utility of the presented design lies in the simplicity of implementation brought by the micro-

controller based platform. IoT devices based on Arduino have been designed in which data has to be accessed by entering the IP address assigned to the device in the web browser [7]. Also, these devices tend to upload only current data [7][8], which does not allow data logging and analysis. In some systems [9], the measured parameters can be read by the user in "on demand" mode. Depending on the type of data, some systems [10] upload data to a Google Spreadsheet and make it privately accessible to the authorized user. Since, the presented device uploads the data to a Twitter account, the data is accessible from anywhere around the world. It can also be made accessible to the general population if required. Followers of the account can be notified of updates. Further, it is possible to maintain record of the past data which can then be analysed to extract knowledge about climate patterns.

III. CONTROL UNIT

The central control unit used in the presented IoT device is the sophisticated microcontroller based platform Arduino Uno R3 (Arduino). The Arduino Integrated Development Environment (IDE) [11][12] is an open-source software package used to program the Arduino using a high level programming language similar to C and C++ through serial communication using a PC. The Arduino used with the Arduino Ethernet shield [13] can be used to connect the Arduino to the Internet.

IV. INPUT DEVICES

4.1. Wired Binary Switch Sensor- Photodiode

The day and night cycle plays an important role in determining trends in weather. Changes in the duration of day and night indicate transitions in seasons. Monitoring of the day and night cycle can also be used to control street lighting automatically. This is an energy efficient system that can be used in smart city projects.

In this case, a photodiode is used to indicate whether it is day or night. The photodiode output is connected to a digital I/O pin of the controller. It acts as a binary switch which senses whether it is day or night. The circuit for the photodiode is shown in Fig.2. The potentiometer R2 is used to set a threshold voltage such that the two distinct states of the photodiode output indicate whether it is day or night. The operational amplifier based comparator gives a binary output depending on the daylight conditions and sends it to the control unit. Due to frequent variation in sunlight and cloud cover, it may be difficult to set a fixed threshold. The seasonal variations can be incorporated using the potentiometer. For the daily variations, the temperature and humidity can be used along with the photodiode output to determine whether it is day or night. This simple circuit can be used effectively in practical applications.

Instead of the photodiode, light dependent resistors (LDR) can be used to analyze more aspects of the day and night cycle with greater accuracy. The amount of (5)insolation received can be monitored through the use of various sensors like LDR. It can help to identify whether the weather is sunny, cloudy, clear, etc. Further, analysis of insolation readings can have significant importance for solar energy applications.

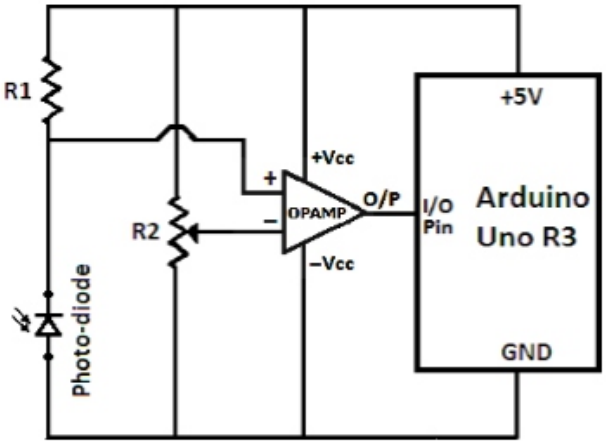

Fig. 2. Photodiode based Day-Night Sensing Circuit

4.2. Wired Analog Sensor- Humidity Sensor Humidity indicates the moisture content in air. As the air gets saturated with moisture, precipitation may occur. Observation and analysis of the humidity readings in a region over a long time can help to understand and thus predict rainfall patterns. Absolute humidity is the content of water in air in gm/m3. Relative humidity is expressed in percentage as the ratio of absolute humidity to the maximum absolute humidity possible at that temperature. When the relative humidity increases, either due to increase in water content or a drop in temperature, the water content in the air condenses to give precipitation. Thus, monitoring relative humidity can help to analyze and eventually predict precipitation patterns.

In this case, the analog humidity sensor SY-HS-220 [14] measures the relative humidity (RH) in percentage. The standard characteristics of the sensor as per the datasheet [14] are nearly linear. Therefore, linear regression analysis is performed as shown in Eq. (1) to approximate the characteristics to a straight line and enable interpolation.

$$Vo = (0.0331\,x\,RH) - 0.0115 \qquad (1)$$

The in-built ADC of the controller converts the analog voltage input Vo to the digital voltage reading V which is converted to relative humidity (RH) by the control unit as shown in Eqs. (2)-(5).

$$V = \left(\frac{Vo}{5}\right) x\ 1023 \qquad (2)$$

$$RH = \frac{(Vo + 0.0115)}{0.0331} \qquad (3)$$

$$RH = \frac{\left(\left(\frac{V}{1023}\right)x\,5\right)+0.0115}{0.0331} \qquad (4)$$

$$RH = (V\,x\,0.148) + 0.3474 \qquad (5)$$

4.3. Wireless Digital Temperature Sensor

Monitoring and analysis of temperature readings in a region over a long time can help to understand seasonal changes and their patterns. Analysis of trends in temperature variation over many seasons can help to understand the impact of global warming and thus, climate change. The temperature and humidity readings together can help to eventually predict precipitation patterns more accurately than by using the humidity reading alone. Temperatures may vary over short distances and short time intervals in a region. Thus, multiple temperature sensors can be connected wirelessly, with a central control unit, over a region to obtain a temperature map.

In this case, the digital temperature sensor DS18B20 [15] is used with a microcontroller based wireless unit. The microcontroller sends the temperature reading serially to the Xbee [16] module for transmission. The reading is received by the Xbee receiver connected to the Arduino. The circuit for the wireless temperature sensing unit is shown in Fig. 3 and the connection of the Xbee receiver to the Arduino is shown in Fig. 4.

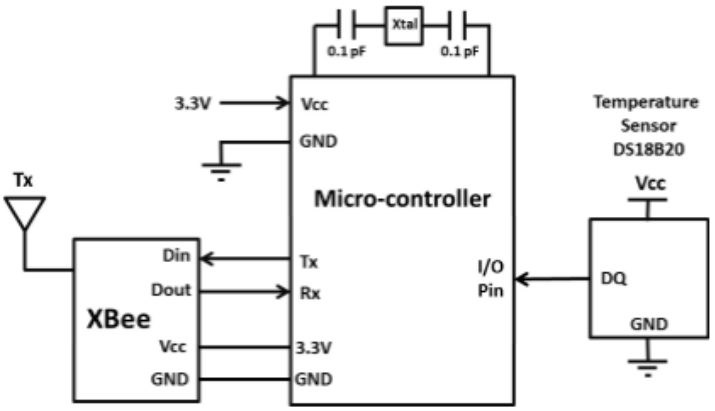

Fig. 3. Wireless Temperature Sensing Unit Circuit

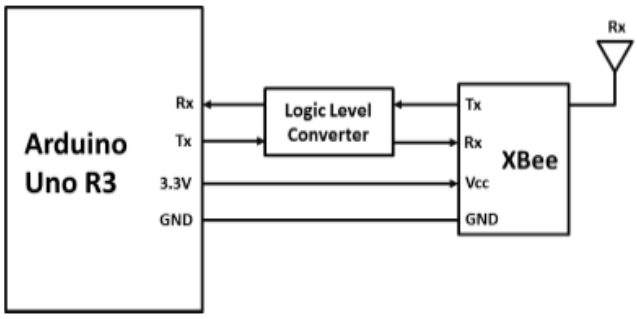

Fig. 4. Connection of Xbee RF module to Arduino

V. OUTPUT DEVICES

Depending on the input received from the photodiode, in this case, a lamp driven by the AC mains is switched on or off using a relay. If it is day, the lamp is switched off and if it is night, it is switched on. The relay circuit for the output lamp is shown in Fig. 5. To prevent any back flow of heavy current from the AC mains into the highly sensitive low power control unit, optical coupling is used for electrical isolation between the control unit and the relay circuit. A diode is used with the relay to block the negative signal from comparator. Similar systems can be used for energy-efficient, automated street lighting in smart city projects.

Similarly, a variety of different sensors can be used to control different output devices for different applications. For example, temperature can be used to control fans, air conditioners and heaters. This can save a significant amount of energy as these are all high power-consuming devices. Motion sensors can be used to detect activity in a room. The lights in the room can be switched on only if the presence of a person is detected. Sensors that measure the moisture content in soil can be used to control the automated irrigation systems. Thus, water can be supplied to the plants only when required and in appropriate quantity. This will conserve water and help to combat the effects of drought. IoT can thus, help to build decision support systems for precision agriculture which is a revolutionary concept in itself.

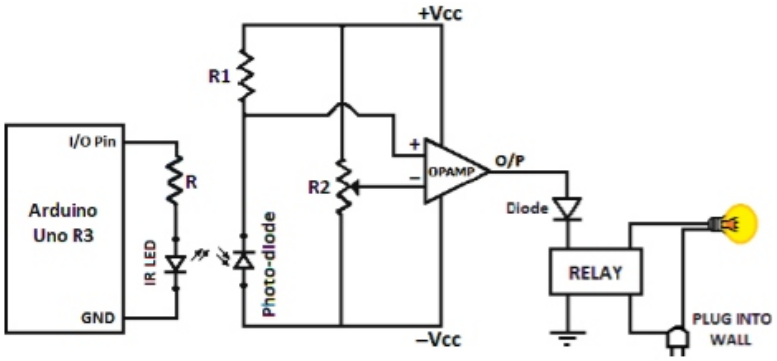

Fig. 5. Relay Circuit for Output Lamp

VI. INTERNET MECHANISM

The Twitter API is a RSS feed. Rich Site Summary (RSS) provides a class of web feed formats that can be used to publish frequent updates in information. The data can also be made available to the general public if required. Thus, Twitter is a convenient Application Program Interface (API) to upload the weather parameters. The collected sensor data is uploaded on an authorized Twitter account.

Twitter uses the HTTP Secure Protocol which uses the SSL encryption layer along with HTTP. The Arduino executes the application layer functions of the IoT device whereas the transport layer, network

layer, link layer and physical layer of the device are implemented in the Ethernet shield. Thus, there is no provision for accommodating encryption layer functionality in this IoT device. Therefore, the Arduino cannot tweet directly. It sends the message to a proxy server http://arduino-tweet.appspot .com/ [17] which runs on the simple HTTP application layer protocol without SSL encryption. The proxy server then tweets to the Twitter account. However, the communication of the Arduino over the Internet in this case is unsecured due to the lack of encryption layer.

Access is authorized by the OAuth [18] token generated for the Twitter account. OAuth generates a token for the given user credentials which in this case are the login details for the Twitter account. This token is used to give Arduino access to the Twitter account, with the permission of the account holder, without sharing user credentials. Thus, the Arduino does not need to specify the user-name and password every time it needs to tweet.

In this case, the Arduino is connected to the internet using the Arduino Ethernet shield [13]. The Ethernet connection can be initialized either by dynamically obtaining the IP address from a DHCP server or manually configuring the IP address, subnet, default gateway and DNS.

The Arduino Tweet Library [17] is used to send tweets using the Arduino. The data gets time-stamped as every tweet is time-stamped by Twitter. Twitter rejects a new tweet if it is the same as the last one and gives a 403 Forbidden status code error. Even though the tweet request is valid, the Twitter server refuses to respond to it. To overcome this, a counter is incremented for every tweet and sent along with the sensor data in case sensor data does not change. A successful tweet gives a 200 OK status code. The function in the Arduino Tweet Library used for sending the message involves making a HTTP POST request using the URL: http://arduino- tweet.appspot.com/update?token=OAuthToken&statu s=data. The OAuth token and the data to be uploaded are embedded in the URL.

By archiving the tweets as a CSV file, it can be possible to represent the data graphically for better understanding of trends from the data. By using more sophisticated cloud platforms for uploading the sensor data, it can be possible to do this analysis in real time. A sample graph for temperature variation is shown in Fig. 6. The graphs of day and night cycle can indicate seasonal variations in the duration of day and night. An increasing trend in humidity can indicate a possibility of precipitation. Trends in temperature change can indicate seasonal variations. When observed over a long time, temperature variations can help to identify the rate of global warming.

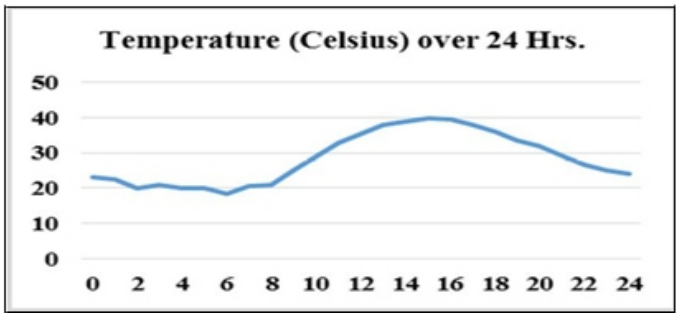

Fig. 6. Graph for Variation of Temperature over 24 hrs.

VII. DESCRIPTION OF ALGORITHM

After initialization of libraries and I/O pins, the photodiode input, temperature input and humidity input are read by the control unit. If the photodiode input is 'high', the relay output driving the output lamp is 'low' and vice versa. The photodiode input is sampled every second to control the output lamp whereas the temperature and humidity readings are taken every minute. Every sixtieth photodiode reading and every temperature and humidity reading are inserted into the format of the HTTP POST request URL for sending a tweet and thus the data is uploaded on Twitter.

VIII. RESULT

The weather parameters, uploaded by the device, are received as updates to followers of the Twitter account. The data can be accessed from anywhere with the aid of an Internet enabled device such as PC, smartphone, tablet, laptop etc. If the data is made public, it can be accessed by searching for the Twitter handle. The uploaded time-stamped weather data is seen in the screenshots shown in Fig.7. A new Twitter notification arrives as per a preset time interval giving details of daylight, temperature and humidity along with a counter. Fig. 8 shows temperature variation due to the presence of heating elements near the temperature sensor.

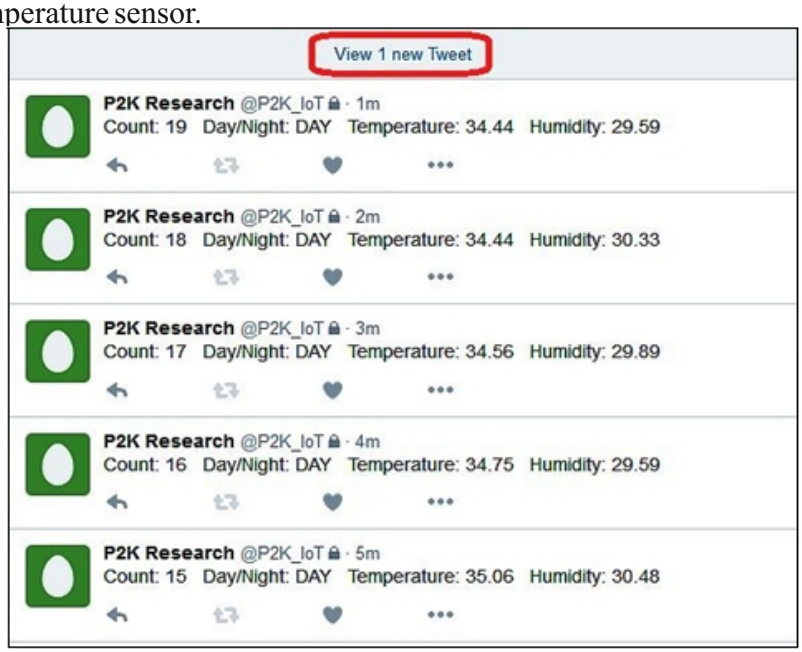

Fig. 7. Output Screenshot of Twitter

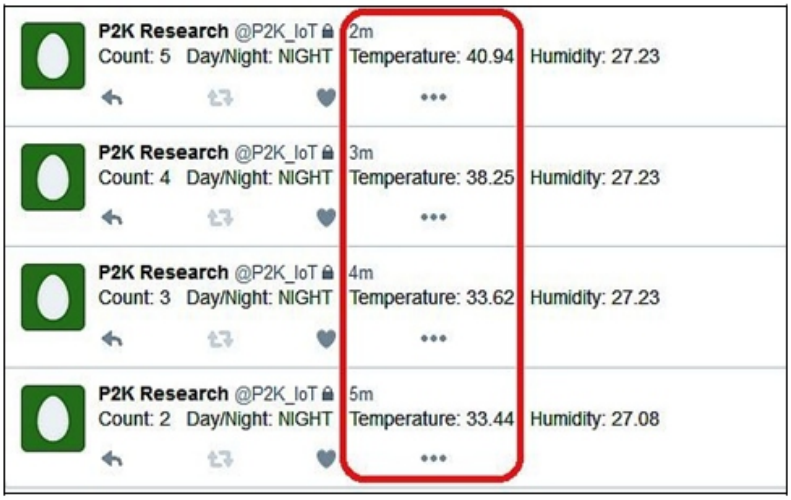

Fig. 8. Occurrence of temperature variations in tweets due to heating over 4 minutes

IX. PERFORMANCE EVALUATION

9.1. Impact of Internet Mechanism on Sampling Rate

The slowest hardware component is the digital temperature sensor DS18B20 with a response time of 750 ms [15]. Thus, the maximum delay generated by the hardware is 750ms. However, sending tweets within an interval of one minute overloads the proxy server [17]. Thus, the uploading mechanism is the slowest component of the entire system and limits the sampling rate to one minute. However, the photodiode is sampled every second to ensure that the relay switch control is not delayed. Every sixtieth reading of the photodiode is uploaded on the Internet.

9.2. Range of Wireless Components in the IoT Device

The range of wireless components determines the range of connectivity of the IoT system. This is an important factor that must be taken into consideration while installing IoT devices in difficult geographical terrains. In the current example, Xbee Series-1 module is used for wireless communication. The range for this module is 30m (approximately 100 feet) as per the datasheet [16].

CONCLUSION

The IoT device based on the presented design can be used to remotely monitor weather parameters like daylight, temperature and humidity. The data can be stored online, which can be used to forecast weather and eventually analyze climate patterns, as well as for other meteorological purposes. The system uses a good combination of analog and digital sensors in wired and wireless modes of operation. Thus, a proof of concept for an Internet of Things device for a remote weather monitoring system has been established. This basic design can be extended and modified suitably to realize other IoT applications as well.

FUTURE SCOPE AND APPLICATIONS

The current product design involved only logging of data. Thus, the device was interacting only with the server side. The functionality of the device can be extended to M2M communication through the Internet. More sophisticated cloud services such as Xively, Nimbits, Google Drive etc. can be used which can provide facilities for real-time graphical representation, analysis and processing of data. A separate cloud instance may also be developed to cater to the needs of the specific application. The communication of the Arduino with the Internet can be made more secure by incorporating encryption and source coding techniques. Provisions can be made in the device to debug its operation. Increased processing power can be obtained, if required, using computationally advanced control units such as Raspberry Pi, BeagleBone Black etc.

Integration of environmental sensors with such IoT devices can help to develop numerous applications [19] for energy conservation and thus sustainable development. For example:

1. Early detection of earthquakes and tsunamis can be done by monitoring seismic activity using sensors without the need to visit the unreachable or unsafe site. This can help in early and effective disaster management operations.
2. Combustion gases and pre-emptive fire conditions can be detected to define alert zones. Similarly, forest fires can be detected at an early stage even though human presence is very less in dense forests.
3. Pollution of air and water can be controlled by monitoring toxic waste in industrial emissions and within industries. This helps to maintain the quality of air and water.
4. Monitoring of items such as medicines, perishable food products in transit can help to ensure the quality of the product delivered to the consumer and reduce wastage of food. This reduced wastage of food can help to ensure food security.
5. Motion sensors can be used to remotely detect wildlife habitat, movement, migration in forests.

IoT devices have significant applications in many fields and thus have a huge potential market. In future, most of the things in the world will be connected to each other through IoT. Thus, it is very important to ensure that the world wide IoT has a robust structure. The issues regarding IoT [20] that need to be addressed are: interoperability of multiple systems, security of data, necessity of standards in IoT, government policies for IoT, increasing computing power to handle the huge amount of data generated by sensors, increasing availability of sensors and actuators to connect things in IoT.

ACKNOWLEDGEMENTS

The authors would like to thank Dr. Mrs. R.D. Joshi, Asst. Professor, E & TC Dept., College of Engineering, Pune for her guidance and support.

REFERENCES

[1] Charalampos Doukas, "Building Internet of Things with the Arduino", CreateSpace Publications, 2012
[2] Shifeng Fang et al., "An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things,", IEEE Transactions on Industrial Informatics , vol.10, no.2, pp.1596-1605, May 2014
[3] Twitter, https://twitter.com
[4] Arduino Uno R3 Datasheet, Available: http://arduino.cc/en/Main/arduinoBoardUno
[5] M. Ibrahim, A. Elgamri, S. Babiker and A. Mohamed, "Internet of things based smart environmental monitoring using the Raspberry-Pi computer," Fifth International Conference on Digital Information Processing and Communications (ICDIPC), 2015, Sierre, 2015, pp. 159- 164.
[6] Raspberry Pi - Teach, Learn, and Make with Raspberry Pi, Available: http://www.raspberrypi.org/
[7] S. R. Mohana and H. V. Ravish Aradhya, "Remote monitoring of heart rate and music to tune the heart rate," Global Conference on Communication Technologies (GCCT), 2015, Thuckalay, 2015, pp. 678-681.
[8] M. Suresh, P. Saravana Kumar and T. V. P. Sundararajan, "IoT Based Airport Parking System," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, Coimbatore, 2015, pp. 1-5.
[9] A. Leone, G. Rescio and P. Siciliano, "An open NFC- based platform for vital signs monitoring," AISEM Annual Conference, 2015 XVIII, Trento, 2015, pp. 1-4.
[10] Kulkarni, P.H.; Kute, P.D., "IoT Based Data Processing for Automated Industrial Meter Reader using Raspberry Pi," presented at the International Conference on Internet of Things and Applications, Pune, India, 2016
[11] Simon Monk, "Programming Arduino- Getting Started with Sketches", Tata McGraw Hill Publications, 2012
[12] Arduino, Available: http://www.arduino.cc/
[13] Arduino Ethernet Shield W5100Datasheet, Available: http://arduino.cc/en/Main/arduinoEthernet Shield
[14] Analog Humidity Sensor SY-HS-220 Datasheet, Available: www.tme.eu/en/Document/d6b8 c0 8f190d39dd5204c1edb 9f c2516/\\sy-hs-220.pdf
[15] Digital Temperature Sensor DS18B20 Datasheet, Available: http://datasheets.maximintegra ted.com/en/ds/DS18B20.pdf
[16] Xbee RF Module Datasheet, Available: www.digi.com/pdf/ ds_xbeemultipointmodules.pdf
[17] Tweet Library for Arduino, Available: https://arduino- tweet.appspot.com/
[18] OAuth 2.0- OAuth, Available: http://oauth.net/2/
[19] Top 50 Internet of Things Applications, Available: http://www.libelium.com/top_50_iot_sensor_ applications_ ra nking/
[20] M. A. Razzaque, M. Milojevic-Jevric, A. Palade and S. Clarke, "Middleware for Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70-95, Feb. 2016

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

Note