JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-5, Issue-4 E-ISSN: 2347-2693

Provenance-Based Assurance Model for Delay Tolerant Network

K. Soni[1], **Prabadevi. B**[2*]

[1]Dept. of CSE, VIT University, Vellore, India
[2]Dept. of CSE, VIT University, Vellore, India

Corresponding Author: prabadevi.b@vit.ac.in, Tel.: +91-7871232823,9442690043

www.ijcseonline.org

Received: 22/Mar/2017, Revised: 02/Apr/2017, Accepted: 21/Apr/2017, Published: 30/Apr/2017

Abstract— Use of End to End connectivity in today's network connectivity is not secure due to its delay and disconnection. This problem can be avoided by the Provenance-based Assurance model proposed in this paper. This model first assures that a node is trustworthy and to whom the data will be sent. It evaluate trust by the information added by the message carrier as indirect clue when message is forwarding. So the problem of disconnection and delay can reduce by this strategy. This model first splits the file into packets then these packets will be encrypted by using DES algorithm with the secret key which is given by sender. After this we will cluster the nodes and send the packets to receiver's end. Receiver will receive the packets and decrypt it using the same secret key which sender use for encryption. After decrypting it, receiver will get the original file content. This proposed system ensures high level of security with low communicational cost and high performance.

Keyword— Delay Tolerant Network, End to End Connectivity, Provenance-based Assurance Model, Disconnection, DES Algorithm, Cluster

I. Introduction

DTN (Delay Tolerant Network) can be found in applications that are coming forth in which many nodes reach to an objective by involving in a group discussion. Example of such applications are - applications where good and urgent response is needed, in different kind of environments, in monitoring activities and in ad-hoc networks.

The main feature of DTNs is that there is no surety of end-to-end connectivity this leads to disruption. This disruption occurs because of the features which are inherent or due to nodes which act in inappropriate manner. To meet the system goals such as - quality, reliability, scalability and availability, trust should be in-charged in an effective and efficient way for providing collusion and decision making works in DTNs. The nodes in DTNs are dispersed scantily so they meet each other rarely. Due to this exchange the nodes cannot be verified. So, disturbingly provocative assessment of trust is most demanding in DTN environment. The absence of undeviating communication in DTN environment creates obstruction in authentication due to which the outcome is inaccurate trust estimation, whose consequence is indigent performance of application. So, we prefer using provenance information for evidence propagation for scantily scattered DTNs instead of using encounter based exchange. Other protocols use encounter based trust but we do not need nodes for exchanging trust evidence while encounter to get approximate trust of the nodes. Hence, attaining high trust exactness by the use of provenance information inserted in a message, when we send message and when it is delivered.

Ameba, is a framework that we are using here for delivery in time. For this we hold the content properties to know the exact routing hop count of every content, in order to increase the number of nodes. Then, we develop node utilities to get the location capacity to get the location, capacity and interest of mobile devices. At last the distributed forwarding schemes holds the exact routing hop count and node utilities to deliver content to the needed nodes at regular intervals. Results had shown that Ameba's delivery ratio can be matched with Epidemic while Ameba does it much faster.

This paper is organized as follows: section II provides the Literature Survey, Section III describes the Proposed System, Section IV describe Implementation, Section V describe Result, Section VI describe Conclusion and Section describe References.

II. Literature Survey

B.MALATHY B.E and S.ROSY ROBILDA B.E proposed E-STAR for building up steady and dependable courses with ALERT in heterogeneous multi hop remote systems. E-STAR consolidates installment and trust frameworks with a trust-based and vitality mindful steering convention. The installment framework remunerates the hubs that hand-off others' bundles and charges those that send parcels. The trust framework assesses the hubs' capability and dependability as far as multidimensional trust values. The trust qualities are joined to the hubs' open key authentications to be utilized as a part of settling on steering choices. By along these lines, E-STAR can invigorate the hubs to transfer parcels, as well as to keep up course soundness and report remedy battery vitality ability. For namelessness ALERT stows away fundamentally source and goal character utilizing pen name changes much of the time. What's more, ALERT likewise shroud course amongst source and goal. With this ALERT additionally having technique against crossing point assaults. Reproduction comes about exhibit that our steering conventions can enhance the parcel conveyance proportion and course soundness.

Mrs. Suvarna L. Kattimani, Mr. Jaeerahmad N. Indikar and Dr Suvarna Nandyal proposed, a Trust administration in portable remote system is dependably been testing a direct result of as often as possible changing system condition. This will bring about postpone resistance systems a high inactivity, visit detachment over problematic remote connections. To maintain a strategic distance from these irregularities they proposed Dynamic Trust and Security Management Protocol (DTSMP).In the present Internet design (IP-based engineering), information are dealt with as system components as a progression of bytes that must be exchanged from a particular source to a particular goal. However, the system components have no learning of the data they exchange a, thus can't understand improvements that would be conceivable (e.g., data replication at different focuses, data mindful movement building, keen in-system storing). To beat these issues they utilize the Information Centric-Networks (ICN) engineering for our proposed DTSM convention. They plan and approve the Dynamic Trust and Security Management convention for postpone tolerant systems (DTN) for better enhanced secure directing in DTN condition; this incorporates very much acted, narrow minded and vindictive hubs. Proposed work is investigated and approved by means of broad reenactment. Their convention decide and apply the best streamlined operational setting at the runtime in light of powerfully changing system condition, by will limit the trust inclination and boost the directing execution. They do similar examination with other trust conventions like Bayesian trust-based convention, DTSM convention (proposed) with IP-based design and DTSMP convention (with ICN engineering). The outcomes exhibit that DTSM convention can manage narrow minded conduct, malevolent, and untrustworthy hubs. It likewise demonstrates that DTSM convention work productively on INC engineering which enhance the execution of DTSM convention. Besides proposed convention can bargain viably with message overhead and message postpone which will build the noteworthy pick up in conveyance proportion.

Reinier-Jan de Lange suggests that in environmental science, sensors are most usually utilized for determining or observing ecological procedures. The perceptions are normally gathered on a for each venture premise, in this way these estimations are frequently copied between activities running at numerous associations. A stage in the correct approach to stay away from this duplication is to present sensor systems, as they not just permit specialists to perform continuous information examination, yet empower sensor information sharing also. In any case, with a specific end goal to make exact determinations or approve new models utilizing this naturally gathered information, metadata should be put away that offers intending to the recorded perceptions. The sensor information created by a sensor arrange relies on upon a few impacts, similar to the setup and area of the sensors or the totals performed on the crude estimations. This sort of metadata is called provenance information, as the birthplaces of the information are recorded. In this proposition, the prerequisites of a provenance mindful sensor system are gathered and a work process is proposed for recording and questioning sensor information and their provenance. A model framework actualizing the work process demonstrates that the proposed approach can successfully prepare sensor information from a few sources, of which the utilization is defended in logical research as the information provenance is known too.

Buneman, Peter, Sanjeev Khanna, and Tan Wang-Chiew with the multiplication of database perspectives and curated databases, the issue of information provenance - where a bit of information originated from and the procedure by which it landed in the database - is ending up noticeably progressively critical, particularly in logical databases where understanding provenance is pivotal to the precision and cash of information. They portray a way to deal with registering provenance when the information of intrigue has been made by a database inquiry. They present outcomes for a general information display that applies to social databases and additionally to various leveled information, for example, XML. A novel part of our work is a refinement between "why" provenance (alludes to the source information that had some impact on the presence of the information) and "where" provenance (alludes to the location(s) in the source databases from which the information was removed).

Provenance has been used to affirm trust, constancy, or exactness of information in many research ranges. Numerous people assessed how provenance information is connected with a work procedure in a Bio-Diversity application. A man proposed a data provenance place stock in model to survey unwavering quality of data and data providers. Same individual displayed an administrator based approach to manage regulating information unwavering quality in framework driven information sharing conditions. Golbeck used provenance information to infer trust in Semantic Web based casual groups. Zhou Bell data provenance counts and request over dispersed streams for reasonable framework duty and criminological examination to update compose security. In any case, the above surveys focused on evaluating steadfastness in information without considering specific framework attack rehearses that may noxiously change the principal messages and bother system goals.

Point to Point Protocol-
In PC organizing, Point-to-Point Protocol (PPP) is an information interface (layer 2) convention used to build up an immediate association between two hubs.

PPP is utilized over many sorts of physical systems including telephone line, trunk line, mobile phone and fiber optic cable connections, for example SONET. Point to Point Protocol is utilized over Internet get to associations. Web access suppliers have utilized Point to Point Protocol for client dial-up access to the Internet, since IP parcels can't be transmitted over a modem line all alone, without a few information interface convention.

Two subsidiaries of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are utilized most normally by Internet Service Providers (ISPs) to set up a Digital Subscriber Line (DSL) Internet benefit association with clients.

PPP is normally utilized as an information interface layer convention for association over synchronous and no concurrent circuits, where it has to a great extent superseded the more seasoned Serial Line Internet Protocol (SLIP) and phone organization commanded principles, (for example, Link Access Protocol, Balanced (LAPB) in the X.25 convention suite). The main necessity for PPP is that the circuit gave be duplex. PPP was intended to work with various system layer conventions, including Internet Protocol (IP), TRILL, Novell's Internetwork Packet Exchange (IPX), NBF, DECnet and AppleTalk. Like SLIP, this is a full Internet association over phone lines by means of modem. It is more solid than SLIP since it twofold checks to ensure that Internet parcels arrive in place. It resends any harmed parcels.

III. PROPOSED SYSTEM

We are proposing a system by which we can reduce the communication cost and increase the message delivery rate. This proposed system will have various techniques like cluster, encryption - decryption and many more. Provenance is the keyword which is the solution of this problem, this algorithm first evaluate the trust of the node by the help of message carrier then send the message. We are adding the clustering which split the whole message in to some packets. These packets will have the data related to that message. Then we encrypt these packets by the DES encryption algorithm. These encrypted packets will go to different nodes and these nodes will send the all packets to the receiver end and receiver will have a private key by which he can decrypt the packets and convert it into message again.

Provenance Model-
The Open Provenance Model (OPM) was acquainted with speak to information provenance, handle documentation, information inference, and information explanation. From that point forward, OPM has been generally received and stretched out by different research bunches. Freire et al. studied different models of provenance administration however did not talk about the utilization of provenance for security. McDaniel tended to that precise, opportune, and point by point provenance data prompts great security choices.

Provenance has been utilized to confirm trust, reliability, or rightness of data in many research territories. Rajbhandari et al. inspected how provenance data is related with a work process in a Bio-Diversity application. Dai et al. proposed an information provenance confide in model to assess reliability of information and information suppliers. Yu et al. displayed an operator based way to deal with overseeing data dependability in system driven data sharing situations. Golbeck utilized provenance data to derive confide in Semantic Web based informal communities. Zhou et al. utilized information provenance calculations and inquiries over appropriated streams for successful system responsibility and measurable investigation to improve arrange security. In any case, the above reviews concentrated on assessing dependability in data without considering particular system assault practices that may perniciously change the first messages and disturb framework objectives.

A few analysts have tried endeavors to secure provenance information. Hasan et al. demanded that safe provenance is a basic perspective to build security of provenance data. Braun et al. clarified that "provenance" comprises of connections (i.e., a chart) and characteristics (i.e., qualities of an element). Hasan et al. exhibited a provenance-mindful model to guarantee honesty and privacy of provenance data in light of provenance following of information composes at the application layer. Wang et al. proposed a "chain-structure" provenance plot that gives security affirmation to provenance meta-information. Gadelha and Mattoso proposed a security design structure that ensures initiation and transient data in matrix empowered provenance frameworks. Lu et al. proposed a provenance conspire utilizing the bilinear matching procedures keeping in mind the end goal to secure provenance information of possession and process history of information question in distributed computing. The above works have considered how to secure provenance information with the presence of a brought together confided in substance.

A few analysts have proposed provenance-based trust models in sensor systems, however they accepted full information of the system topology, and did not consider assault practices.

Clustering-

A PC group comprises of an arrangement of freely or firmly associated PCs that cooperate so that, in numerous perspectives, they can be seen as a solitary framework. Not at all like matrix PCs, PC bunches have every hub set to play out similar assignments, which are controlled and booked by programming.

The parts of a group are typically associated with each other through quick neighborhood ("LAN"), with every hub (PC utilized as a server) running its own occurrence of a working framework. As a rule, the greater part of the hubs utilize a similar equipment and the same working framework, in spite of the fact that in a few setups (i.e. utilizing Open Source Cluster Application Resources (OSCAR)), diverse working frameworks can be utilized on every PC, or potentially extraordinary equipment.

They are generally sent to enhance execution and accessibility over that of a solitary PC, while ordinarily being a great deal more financially savvy than single PCs of equivalent speed or accessibility.

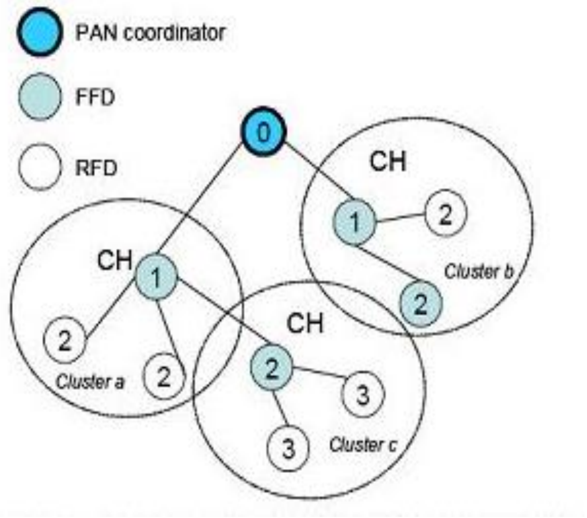

Figure1: Clustering with Multiple Nodes

DES Algorithm-

DES (Data Encryption Standard) is the prototype block cipher— an algorithm that takes a settled length string of plain text bits and changes it through a progression of confounded operations into another figure content piece string of a similar length. On account of DES, the square size is 64 bits. DES likewise utilizes a key to alter the change, with the goal that decoding can evidently just be performed by the individuals who know the specific key used to encode. The key apparently comprises of 64 bits; be that as it may, just 56 of these are really utilized by the calculation. Eight bits are utilized exclusively to check equality, and are from there on disposed of. Consequently the viable key length is 56 bits.

Those key that nominally put away or transmitted as 8 bytes, every with odd equality. One sting within each and every 8 bit byte regarding the accomplishment execute stand utilized because error detection between key generation, distribution or garage. Bits eight, sixteen,…., sixty four are for utilizes of making sure to that amount each byte is regarding unusual parity.

- We isolate the 56-bit key to two 28-bit keys: Lk and Rk
- "Left Shift" the Lk and Rk as indicated by SRT (Sub key Rotation Table)
- After shifting, add Lk and Rk.
- Change as indicated by Permuted Choice.
- Now we have a 48-bit sub key.
- Rehash the operation 16 times to get 16 sub keys
- Use shifted Lk and Rk.

This is the algorithm of DES encryption. Here is diagram given below by which we can understand this algorithm very easily

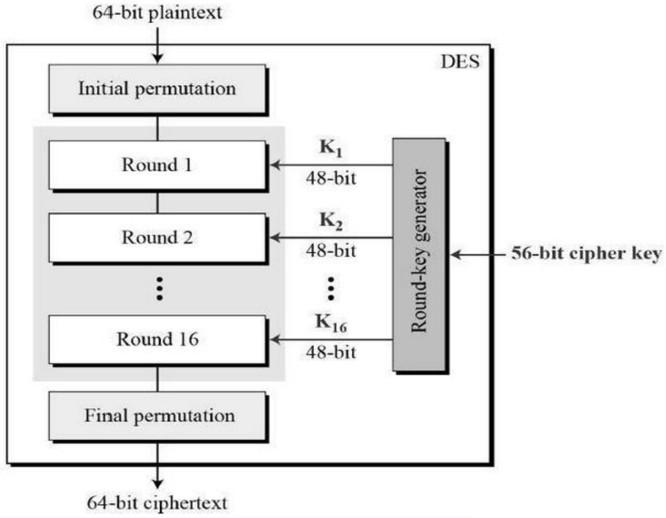

Figure2: DES Algorithm Process

System Architecture-

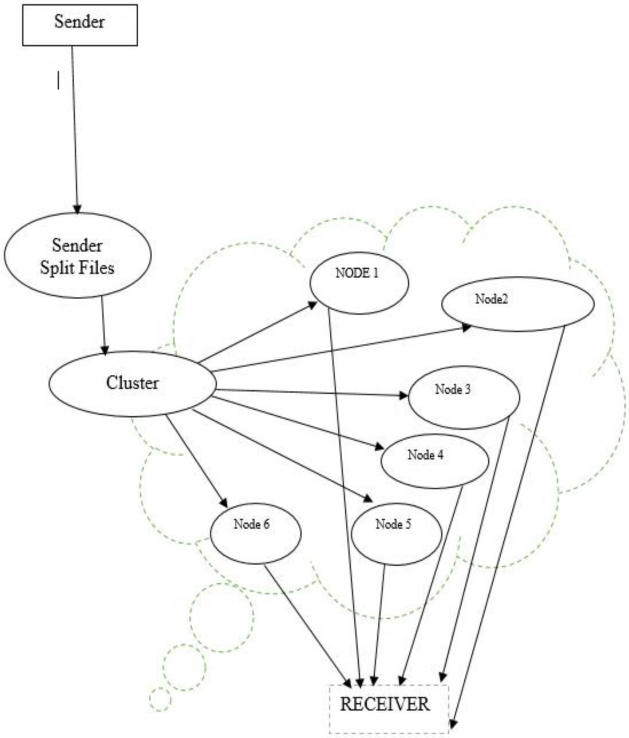

Figure3: Proposed System Architecture

In system architecture, there is a user who will login into the system then he will select a text file which he want to send. Then he will split the file in to packets according to their size. Then he will go directly to next step which is encryption. In this phase he will encrypt that packets by the DES algorithm. Then next phase will come which is clustering the node. Then he will send that packets to the nodes. Each node will have a packet and each node will send their packets to the receiver. Receiver will collect that packets and decrypt them.

To promote content towards required hubs over a DTN in an opportune way, Ameba precisely modifies the quantity of experiences and the quantity of substance duplicates for publicized substance, create sending utilities to catch interests, portability designs, limit imperative and visit areas of cell phones with low support cost, and configuration disseminated transfer calculations to choose the best hubs as the bearers. By means of broad tests, our assessment exhibits that the proposed Ameba plan can accomplish high conveyance proportion and fundamentally low overhead.

Advantage-

1. It will improve the delivery rate of message.
2. It will also decrease the cost of communication.
3. Packet loss also decrease by the proposed architecture.

IV. Implementation

Implementation of this proposed system is done in java language. We use Eclipse software for the implementation. These all are for front end. For the back end, we use MySQL. The data of sender or receiver will store in the MySQL. The user interface is quite simple and very easy to understand.

In this process, first we have to make a user interface for registration and login. If user is not registered than he have to register or if user is registered than he will go to login. After login he will have to go to home page where he will have to select any file which he want to send than it will encrypt by using DES algorithm and send to the other end.

This is the short description of the implementation. For implementation, we use techniques like split file into packets, encryption-decryption and clustering.

V. Result

The proposed system is more consistent, secured and higher delivery rate. Previous protocol is point to point which is not secure and also not consistent, the communication cost of this protocol also high. This system is on Provenance model which doesn't carry this drawback in wireless network communication. The graph can shows the performance of the system.

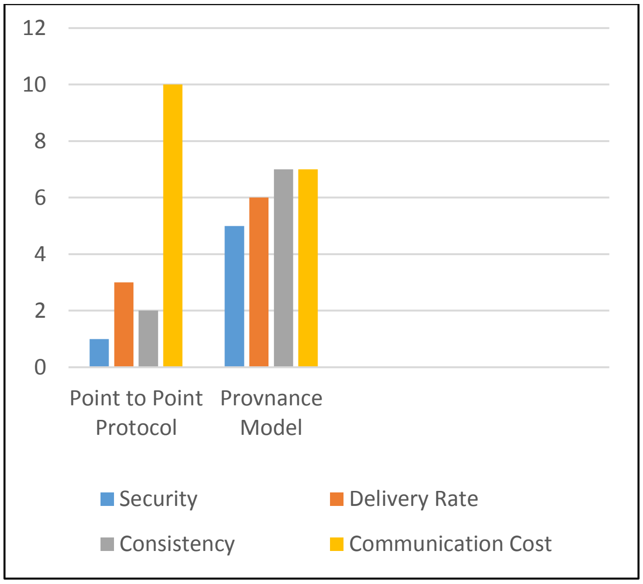

Figure4: Graph for the Comparison between Existing and Proposed System

This graph shows the difference between the existing system and proposed system. Proposed system is better than the existing system.

VI. CONCLUSION

We are proposing a model which can prevent delay occurred in point to point network because of traffic among nodes in a network. Existing technique was End to End Connectivity. This technique is the reason of delay in any network because it simply sent the file to receiver which is sending by the sender.

But this model first use clustering methodology then encrypt the data by DES algorithm. So, data theft will be avoided and there also will not any delay in network because of clustering because all nodes will do same work so there will not be traffic.

In brief, we can say that the proposed system will help to prevent the delay and any crime like data theft.

VII. REFERENCES

[1] Cho, Jin-Hee, Ray Chen, "*PROVEST: Provenance-based Trust Model for Delay Tolerant Networks*", IEEE Transactions on Dependable and Secure Computing, Vol. PP, Issue.99, pp. 1-1, 2016.

[2] B. MALATHY , S.ROSY ROBILDA, "*Secure and Reliable ESTAR with Alert Protocols for Heterogeneous Multihop Wireless Network*", International Conference on Emerging Engineering Trends and Science, Vol. 26, Issue.4, pp. 1140-1153, 2016.

[3] M.Arshiya Shajareen, S. Vasundra, "*Trust and Security Management Protocol for Delay Tolerant Networks Using Information Centric Network Architecture (ICNA)"*, International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.6-11, 2015.

[4] P. McDaniel, "Data provenance and security", IEEE Security and Privacy, Vol. 9, Issue.2, pp. 83–85, 2011.

[5] Reinier-Jan DeLange, "Provenance Aware Sensor Networks for Real-time Data Analysis", Master thesis from University of Twente, Netherlands pp.1-220, 2010.

[6] T. Spyropoulos, R. Rais, T. Turletti, K. Obraczka, A. Vasilakos, "Routing for disruption tolerant networks: taxonomy and design", Wireless Networks, Vol. 16, No. 8, pp. 2349–2370, 2010.

[7] Aldeco-Pérez, Rocío, Luc Moreau. "*Securing provenance-based audits*", In International Provenance and Annotation Workshop, Berlin Heidelberg, pp. 148-164, 2010.

[8] R. Hasan, R. Sion, M. Winslett, "The case of the fake picasso: preventing history forgery with secure provenance", in Proceedings of the 7th Conference on File and Storage Technologies, Berkeley, pp. 1–14, 2009.

[9] L. Moreau, J. Freire, J. Futrelle, R. McGrath, J. Myers, P. Paulson, "The open provenance model: an overview", in International Provenance and Annotation Workshop, Utah, pp. 323-326, 2008.

[10] Zhou, Runfang, Kai Hwang, "*Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing*", IEEE Transactions on Parallel and Distributed Systems, Vol. 18, Issue. 4, pp. 460 - 473 2007.

[11] J. Golbeck, "Combining provenance with trust in social networks for semantic web content filtering", Provenance and Annotation of Data, USA, pp. 101-108, 2006.

[12] Yeo, Jihwang, David Kotz, Tristan Henderson, "*CRAWDAD: a Community Resource for Archiving Wireless Data at Dartmouth*", ACM SIGCOMM Computer Communication Review, Vol. 4, Issue.4, pp.12-14, 2005.

[13] A. Lindgren, O. Doria, "Probabilistic routing in intermittently connected networks", ACM SIGMOBILE mobile computing and communications review, Vol.7, Issue.3, pp.19-20, 2003.

[14] Li. Xiong,, L. Liu, "*Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities*", IEEE transactions on Knowledge and Data Engineering, Vol. 16, Issue. 7, pp. 843-857, 2004.

[15] AA. Selcuk, Ersin Uzun, PM. Resat, "*A Reputation-Based Trust Management System for P2P Networks*",. IEEE International Symposium on Cluster Computing and the Grid, USA, pp. 251-258. IEEE, 2004.

[16] J. Golbeck, JA. Hendler, "*Reputation Network Analysis for Email Filtering*", Conference on Email and Anti-Spam (CEAS), USA, pp.1-14, 2004.

[17] R. Ismail, "The beta reputation system", in Bled Electronic Commerce Conference, Slovenia, pp.1-14, 2002.

[18] P. Buneman, S. Khanna, W. Tan, "Why and where: A characterization of data provenance", in Proceedings of International Conference on Database Theory, Springer-Verlag, pp. 316–330, 2001.

[19] O. Pourgalehdari, M. Salari, "*A Review on Data Aggregation Protocols in Wireless Networks*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.3, pp.50-56, 2017.

Authors Profile

Mr. Krishna Soni pursed Bachlor of Computer Application from Dr. Virendra Swaroop Institute of Computer Studies, Kanpur in year 2015. He is currently pursuing Master of Computer Application from VIT University, Vellore. His main research work focuses on Network Security, Cryptography Algorithms and privacy in communication.

Prabadevi B is an Assistant Professor at VIT University. She completed her under graduation and post-graduation under Anna University, Chennai in 2010 and 2012. She is currently pursuing her research at VIT University, Vellore in the area of /network Security attacks. She has published research papers in international conferences and journals of repute.