A Study about Behaviour of Nodes in Trust Model in Internet of Things

Shweta[1]* Dr. Sunil Kumar[2]

[1] Research Scholar, Department of Computer Science, GJU, Hissar

[2] Assistant Professor, Department of Computer Science, GJU, Hissar

Abstract – In this paper, IOT with application of IOT has been explained. IoT Stands for Internet of things. It has formulated as an essential part of our daily life. IOT is any device or thing which is connected to the internet direct or indirect way. This paper also considered the challenges, limitations and scope of IOT. There is one element the trust which is necessary between user and service provider. The behaviour of nodes in trust model has been mentioned here. This paper includes the different type of attacks. There are several existing researches related to IOT and trust management which have been made in this field also mentioned in this paper.

Keywords: Internet of things, Automation Trust Management

- X -

I. INTRODUCTION

IoT Stands for Internet of items that has become an important component of the day of ours to day life. IOT stands for just about anything or device that is indirectly or directly connected to the web. The word elements include mall devices as cell phones, wearable devices, RFID tags, and sensors and in addition include huge devices as automobiles, big autos, robots etc.

The primary idea of IoT is going digital therefore individuals get comfortable atmosphere where info sharing is hushed simple job and everybody is interconnected. The connection could be between people people, things-things, and people-things. Electronic India is an innovative concept of phone system. In addition, AMRUT (Atal Mission for Rejuvenation, and urbanized Transformation) is created in India for offering simple IOT. and services To be able to interconnect everyone, one have to have a virtual room or maybe the cyberspace whereby cities will be visualized as being a geographical link of individuals, services as well as the activities of theirs just where they are able to perform the day to day activities of theirs such as internet shopping, health care, gaming, wise learning etc. Smart city happens to be an application of IoT wherein an impressive website link is created between technology, electronics, physical equipment and individuals all around.

II. APPLICATIONS OF IOT

This technology had wide range of applications within in different fields. Below are a few possible places where we can use power of Internet of Things to fix regular issues.

Sensible Cities

The web of items might be utilized to observe vibrations of buildings, monuments and bridges in case developing material is threatened or maybe overloaded. Noise pollution might be managed around schools and hospitals. It might be used to manage traffic particularly during traffic jams, accidents, peak hours, rains. It might be utilized to control street lights automatically turn them from inside presence of sunshine & turn them on at beginning of darkness. Yet another helpful program is alerting officials to empty trash containers when loaded within waste.

House Automation

The web of things might be utilized to remotely control & system appliances within the house of yours. It might be helpful in detecting & staying away from thefts Home automation is practice of controlling home appliances instantly working with several balance method methods. Electronic and electrical appliances within home , for example fan, kitchen timer, fire alarm, outdoor lights, lights, etc. may be controlled by using different control strategies. Manufacturing Automation

By utilizing this technology, we might automate manufacturing procedures remotely. It might additionally be useful in optimizing manufacturing processes. We might deal with inventory & supply chain. We can also diagnose whether machines require maintenance and repair. We might monitor emission of deadly gases to stay away from harm to workers' environment and wellness.

Health Monitoring

We might make use of this technology to identify health issues. Patterns of heart rate, pulse, digestive system & blood pressure may be administered & identified for anomalies. Information could be delivered to physician for analysis. Clinic may also be contacted in times of emergency situations. This system will be very helpful to disabled people and elderly people who live independently.

III. CHALLENGES AND LIMITATIONS

Internet of Things accompanies 3 major concerns are over reliance on technology breach of secrecy & job loss. Everything generally stays there when it's put on internet. You will find security measurements [one] which are utilized for protection of info, but a chance of hackers breaking into program & stealing info usually remains there. For instance, Anonymous is the fact that group of people who hacks in federal websites & launch all confidential info in public. In case every one of info is positioned on web, people are able to hack it, & could discover all in regards to a people living Companies could misuse info which is given to log onto it. Lately Google has caught using info that had been private. Data, like information collected & stored by IoT, may be vastly helpful to businesses.

IV. LITERATURE REVIEW

You will find numerous investigations that are produced in this specific area which happen to have provided below: Younghun Chae, et al. [1] wrote on trust management for protecting on off attacks. In this particular paper, they've explained the trust arrangement process.

Farhad Firoozi, et al. [2] discussed the subjective logic based in network information processing. This particular processing is performed for trust control within collocated and sent out WSNS. At the evaluation time period of volatile information gathered in wireless sensor networks of today (WSNs), the disused information in the sensed information needs that it needs to arrange.

Farhana Jabeen, et al. [3] did research on Trust as well as Reputation Management in Healthcare Systems. In addition to this they described the Taxonomy, Open Issues as well as Requirements. In setting of health care, the Trust is viewed as a salient component. That's categorized by doubt and also by a chance component. It's been regarded as a fundamental necessity for the endorsement as well as acceptance of revolutionary solutions about to health care. Smooth faith, trusted social manage strategies has made to evidence based trust agreement. Here the stage of trust is certainly computed with trust engine which is termed as loyalty as well as reputation product (TRS).

Yi Ren, et al. [4] proposed a novel review to Trust agreement. It was concerning to unattended wireless sensor networks. Unattended wireless sensor networks are classified by considerable era of detached purpose.

Renjian Feng, et al. [5] explained a trust analysis algorithm. it's identified in comparison of wireless sensor networks. This kind of WSN is determined by Node Behaviours in addition to D-S Evidence Theory. For WSNs, lots of elements, including mutual interference of wireless links, nodes as well as battlefield programs talked about the earth having not enough excellent actual physical protection.

Fenye Bao, et al. [6] recommended on Hierarchical Trust agreement in case of Wireless Sensor Networks. Additionally they discussed the uses serotonin just in case of trust Based Routing along with Intrusion Detection.

Daojing He, et al. [7] published exploration on Lightweight and attack-resistant Trust Management. Study concentrates on Medical Sensor Networks. Wireless healthcare sensor networks enable ubiquitous health monitoring. Maintain confidence among distributed community entities has recognition as an effective device.

Riaz Ahmed Shaikh, et al. [8] proposed Trust Management problems providing of Distributed Wireless Sensor Networks. The majority of proposed treatments are made on supposition of a faithful system which have the absence of practical.

Tanveer A Zia[9] discussed Reputation reliant Trust Management providing of Wireless Sensor Networks. Wireless sensor networks shows capability in future of many flexible functions.

Bin Ma [10] wrote on Cross layer trust version parallel to algorithm of Node Selection in Wireless Sensor Networks. Nodes help one with transitory of info. These regulate the packets from a single to the next in case of Wireless Sensor Networks Corrupt. Nodes are effectively handled.

S.Karthik, et al. [11] discussed the analysis of Trust Management Techniques in WSNs. They mentioned that WSN as a system comprising multiple affordable sensor nodes. Study concentrates on unstable instances when sensors are powerless to perform certain job.

Chen et al. [12] [13] [14] measured trust composition using QoS along with cultural confidence both. Use of electricity, end-to-end packet forwarding ratio is employed as well as the ratio of package delivery is to calculate the QoS trust [12].

Martinez-Zulia and Skarmeta [15] propose a method of indirect trust aggregation by utilizing credibility that is exclusively produced from the interpersonal QoS and Trust trust.

Josang et al. [16] described node opinion in an additional node in very subjective reason by examining huge aggregation methods including the weighted sum, fuzzy logic, Bayesian inference as well as its idea discounting, trust concept, and regression analysis. Direct trust with self observation may be aggregated with the indirect trust (are generally from colleagues, recommendations along with suggestions), using weighted amount for exactly the same trust attributes.

Saied et al. [17] proposed a method to derive total trust importance by altering the fat that are connected with the all good feedback as well as recommendations. A centralized database is handled by having trust info of IoT entities and eventually just extremely competent IoT products are selected for responding to a service request.

Y.B.Saied et. al. [17] proposed an innovative system for trust management specifically for IoT. The product was created by considering all previous experience and also by regrouping them into sole matric.

Wang et al. [18] proposed a rating technique by considering competence as the main trust matric. Both integrity and competence are believed to be as primary properties for rating. Additionally 2 scaling schemes are used together with the threshold value.

Sharma et.al.[19] presented a pervasive trust management framework for internet personal community.

Golbeck et. al.[21] Developed the algorithm for trust structure that is dependent on the evaluation of previous encounters. The trust is recognized as and computed in social networking and the applicability of its is described.

Z.Lin, L. Dong et. al.[26] created a trust type for societal IoT by incorporating elements as mutuality among requestor as well as service provider, transitive property of loyalty ,.

Daubert et. al.[23][24] created an unit which utilizes trust and keep the security in social IoT. Each service provider is related with a trust factor but together with it an unique care.

Duan et. al.[25] thought the power element while calculating the confidence in IoT.

B.Tian et. al. [27] gave a mathematical formula for computing the confidence in B2C e commerce and classified the standing in e commerce.

H. Zhang, [28] approached trust computation in e commerce by performing computation in two parts. For starters linear trust is estimated by considering three primary dimensions of service i.e. group, transaction Time as well as total.

F. Bao, [29] created the loyalty management protocol in compelling IoT atmosphere that's sustainable, adaptive, and scalable.

Chao et. al. [30] designed security architecture for internet of items together with the idea of press conscious site traffic.

Nitti et al. [31] proposed the trust composition working with quality of service trust by utilizing transaction effectiveness as a measure for QoS trust.

TRUSTMANAGEMENT

One effective component of human and the social relationship of its is Trust. Believe shows the confidence level associated with a specific entity conduct in a particular fashion, in spite of the shortage of capability to manage and monitor the planet in which it works. Believe plays a really crucial job between a service provider as well as a client.

Trust allows in development of standing of the service provider [1] [10] [11]. Besides, it boosts the effectiveness of system and cuts down on the Risk Factor to an excellent extent. Uncertainty factor is decreased with the chance. Trust needs numerous kinds of models depending on the foundation if trust which could be the different disciplines with various kinds and the properties of theirs. Every step consists of different attributes and properties. We want a little algorithm also to assess trust in several stages.

- **Trust origin:** Mostly in each and every discipline, Trust play a vital role. Thus Trust could be originated from Computer science, Sociology etc, Psychology. In computer science, trust could be classified as System as well as User. In the majority of the internet system including Amazon and Flipkart, Trust hinges in the Reviews as well as responses of the current pc user as well as the interaction of theirs in between the participants. Therefore confidence is relational. In websites that are internet, confidence is categorized as: - Direct and Recommendation trust. Immediate trust is dependent on the immediate experience together with the service provider whereas in Recommendation, trust is created on the comments of various other individuals in the system. Inside Recommendation, trust propagates from a single part to the next.

- **Trust Facets:** The kind or trust features of confidence might be Calculative, Emotional, Relational, Cognitive, and also Dispositional, Institutional etc. calculative trust is typical in organizational science and it is based at the statistical calculation of the loyalty. While relational trust is the extended trust created with the constant interaction of trustee together with the trustor. Right here the existing trust is exclusively dependent in previous reliability as well as dependability of the trustor with the good expectations from the trustee. Also referred to as the immediate trust. The psychological trust is the immediate outcome of the connection. Cognitive trust is the based upon the logical action and the cause of its.

- Trust attributes: different trust attributes are context certain, Dynamic, Propagative, Non Transitive, Subjective, Asymmetric, Self reinforcing, Event vulnerable etc. of context specific, trust is dependent on particular context, like, Sachin trust Akshi as a physician but do not believe in her as a technician. Powerful trust keeps on changing with new experiences as well as time. Propagative trust moves from one individual to another transitive in nature. Very subjective trust is dependent on the recommendation as well as review of specific individual. Event very sensitive trust is based on one occasion. Actually a long termed trust is damaged by an individual high impact occasion.

- Trust evaluation: trust is examined based on factors that are numerous. We are able to evaluate trust by providing ranking, scaling, recommendation, formulas etc.

Trust management systems are recommended as shelter mechanism in wireless senor networks. Trust management system may well be utilized to check malicious, selfish, and faulty node. Trust score of information item might be utilized to make serious decisions. Trust management scheme handles anxiety about regarding upcoming performing of nodes. The information as well as node trust designs are categorized in following categories

The centralized trust design calls for centralized reliable authority also often known as base station. It's checking trust report in case of node alongside information product. Centralized TMS haven't been considered appealing for big sensor networks due to resource consumption throughout transmission. Additionally they consume maximum resources during exchange as well as evaluation of trust score.

Distributed Trust design let each node in community to assess trust score themselves for various other nodes. But Distributed trust design isn't considered ideal when there's requirement to establish the upgraded trust rating for various other nodes. There aren't any risks of failure that is the reason it's been recognized as more reliable than centralized trust version. But the limitation of its is more resource usage. This kind of scheme has been known as entirely distributed mechanism. To be able to reduce use of aid the localized distributed trust designs are released. Right here nodes will preserve neighbours trust scores just. Limitation in case of localized distributed trust design is it requires more hours in evaluating trust score of distant node.

The crossbreed trust management takes advantages of both centralized as well as distributed trust version. It offers the gain of decreasing source utilization that's been linked with analysis of confidence in case of distributed solution. Crossbreed strategy continues to be viewed more reliable as compare to centralized trust version. Though it's discovered much less dependable as compare to sent out trust version. Hybrid scheme continues to be used with centralized reliable server. Here the node is analyzing as well as having a single neighbors trust score. It's delivering minimum use of mind as compare to distributed mechanism.

Hence it's realized that entirely distributed and entirely centralized trust design haven't been thought suggestible in case of wireless sensor system. Just in case of centralized information trust version trustworthiness of sensed information products has been examined at centralized server from method perspective.

We have seen a few hybrids, distributed as well as centralized trust type in existence but several schemes aren't able to build communication trust, a few unit failed in establishment of information trust, In certain product there's not enough interdependency while some designs aren't offering security to trust type from strike.

Table 1 various trust management

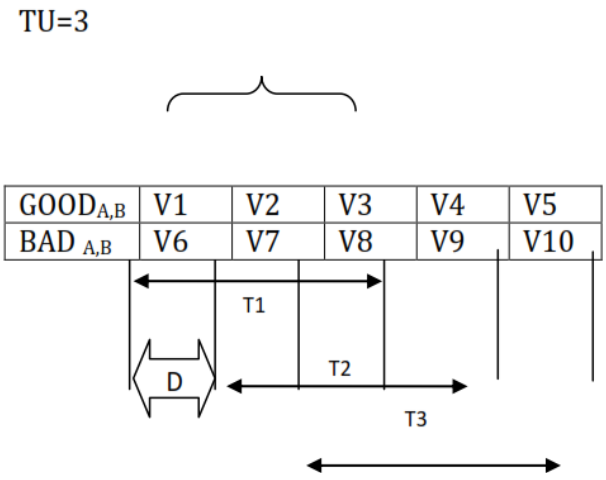
TMS Scheme	Architecture	Com. Trust	Data trust	Inter Dependency	Limitation
ACDT	Hybrid	Y	Y	N	Only spatial correlation is used for data trust
DTMS	Distributed	Y	Y	N	Threat of spoofing attack
MULTIPRO	Distributed	N	Y	N	Threat of attack on trust model
EDTM	Distributed	Y	Y	N	Need to define threshold
DBTA	Centralized	N	Y	Y	No communication trust
ML-TRUST	Distributed	Y	N	N	Trust sharing is missing
LDTS	Hybrid	Y	N	N	Threats of attack
TBFTDA	Centralized	Y	Y	N	Threat of attack on trust model
MDETM	Hybrid	Y	N	N	Need of multi dimension evidence
GTMS	Hybrid	Y	N	N	Threat of attack on trust model

VI. BEHAVIOUR OF NODES IN TRUST MODEL

Node A will estimates trust importance of node B following each D period. It's determined by info that's been recorded on time window TW.

Following Figure represents that after each D time period, period window is sliding to side that is right. It's recording info that is current. In addition to this it's likewise forgetting old information.

Time window in observing figure has 3 time units (TU=3). BADA, B and GOOD A, B are thought bad and good behaviour, respectively, of node B which is noticed by node A. this particular observation is within time window TW.



TU=3

$GOOD_{A,B}$	V1	V2	V3	V4	V5
$BAD_{A,B}$	V6	V7	V8	V9	V10

Considering information in time window TW, trust value of node B according to node A has been represented by following equation

T_{AB}=

$$100x\ (GOOD_{AB})^2/((GOOD_{AB}+BAD_{AB})(GOOD_{AB}+1)))$$

VII. ATTACKS

Many factors are there that affect the trust. There are several types of attacks that become the hindrance during the trust formation. In order to construct a strong trust, one must deal with these attacks. They are categories in various forms; some of them are shown in following figure. While building and computing trust, these attacks must be considered.

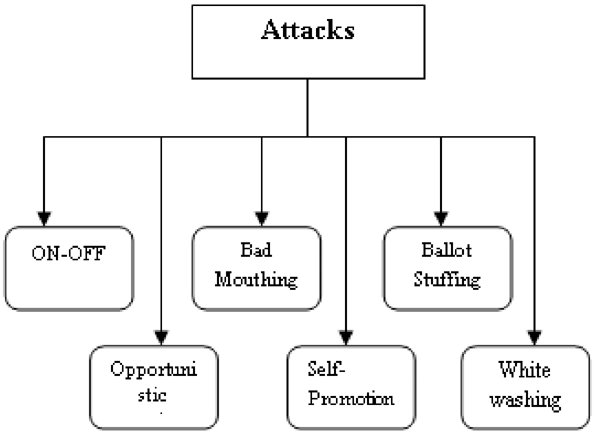


Figure1. Types of Attacks

Nowadays, IoT has connected an extremely big number of objects in world that is real. These items composed of sensors, PDA, smart phones, RFID tags etc. IoT isn't merely restricted to the real life though it's just as effective in virtual world too by joining different virtual items in cyberspace [10]. These may be virtual desktop on the cloud as well as information connectivity [8] [5] [6].

On Off Attack

An attack cycle is described as "on" immediately followed by an "off". If the strike is on, the malicious node launches hits, and also throughout the off time, both stops doing something and even just works well.

Ballot Stuffing

Ballot stuffing is a kind of electoral fraud by which a person permitted just one vote submits many ballots. It is able to additionally occur when someone rather than casting votes in one booth casts his/her vote in several booths.

Opportunistic Service

At an impressive but helpful level cyber-attacks against organisations will be categorised as specific or opportunistic. Identifying that is a useful initial step of understanding and responding to an info security incident. A targeted strike generally involves intelligent preparation and occurs when an assailant selects as well as engages a certain target to attain a certain objective

Self-Promotion

Self-Promotion is a kind of motivation which works in order to make individuals feel great about themselves and also to maintain self-esteem. This particular motive gets particularly visible in cases of threat, hits or maybe failure to one's confidence. Self-Promotion entails a preference for good over bad self-views.

Whitewashing Attack

A whitewashing attack happens when an "attacker resets a bad track record by rejoining the device with a brand new identity."

Look for Trust Computation: You will find numerous dimensions of confidence which help in measurement as well as computation. These're clarified with the aid of following figure. IoT has applications from e health [9] to smart city such as smart communities as well as smart house [7].

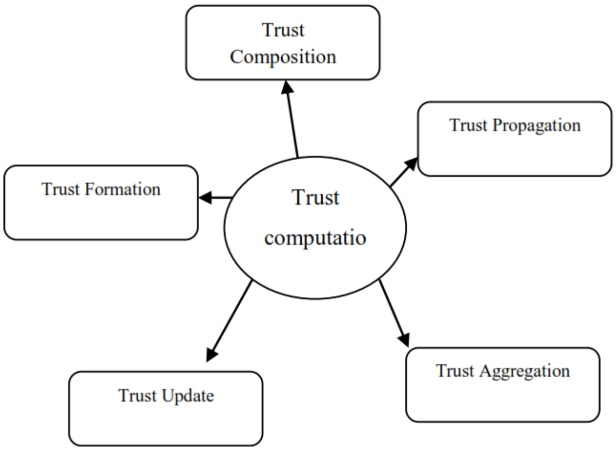


Figure 2 various design dimensions for trust computation models

VIII. SCOPE OF IOT

IOT has numerous advantages into the lives of ours that might help individuals, business and society on daily basis. The brand new idea of its could be presented in numerous forms including safety, financial matters, health, & preparation of each day. IOT Integration in healthcare system is usually really advantageous for both single & society.. Hospitals are already fighting to determine & caring of individuals that they've it gives them power to determine who requires main interest just by monitoring individual's overall health. IOT is able to help people in the private safety of theirs. ADT is a house security system, which allows people in checking the security systems of theirs at home by the phones of theirs, with power to control. In computer science, trust could be classified as "System" as well as "user". In the majority of the internet system including Amazon and Flipkart, Trust hinges in the Reviews as well as responses of the current pc user as well as the interaction of theirs between the members. trust is typical in organizational science and it is based at the statistical calculation of the loyalty. The crossbreed trust management takes advantages of both centralized as well as distributed trust version. It offers the gain of decreasing source utilization that's been linked with analysis of confidence in case of distributed solution.

REFERENCES

1. Dong Chen TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Computer Science and Information Systems, Vol. 8, No.4.

2. I. R. Chen, J. Guo, F. Bao (2014). "Trust Management for SOA-based IoT and Its Application to Service Composition", IEEE Transactions on Services Computing, Vol.99, pp.1-14.

3. R. Venkataraman, M. Pushpalatha, T. Rama Rao (2014). "Logit Trust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks", 6th ASE International Conference on Privacy, Security, Risk and Trust.

4. J. Guo, I.R. Chen, J.P. (2017). “A Survey of trust computation models for services management in internet if things System”, computer communications, Vol-97, pp. 1-14.

5. M.R. Rahimi, N. Venkatasubramanian, S. Mehrotra (2012). Applications on an Elastic and Scalable 2-Tier Cloud Architecture, IEEE/ACM Fifth International Conference on Utility and Cloud Computing, pp. 83-90.

6. Y.B. Saied, A. Olivereau, D. Zeghlache, M. Laurent (2013). "Trust management system design for the Internet of Things: A context-aware and multi-service approach", Computers and Security, Vol. 39, pp. 351 365.

7. Y. Wang, I.R. Chen, J.H. Cho, A. Swami, K. Chan (2016). "Trust-based Service Composition and Binding with Multiple Objective Optimization in Service-Oriented Mobile Ad Hoc Networks", IEEE Transactions on Services Computing.

8. J.Granjal, E. Monterio (2015). “Security for the internet of things: A survey of existing protocols and open research issue”, IEEE

Communications Surveys & Tutorials, Vol. 99, pp. 11.

9. A. Jøsang (2002). “The Beta Reputation System”, Proc. 15th Bled Electronic Commerce Conf., pp. 1- 14.

10. I. R. Chen, F. Bao, J. Guo (2016). "Trust-based Service Management for Social Internet of Things Systems", IEEE Transactions on Dependable and Secure Computing.

11. M. Nitti, R. Girau, L. Atzori (2014). "Trustworthiness Management in the Social Internet of Things", IEEE Transactions on Knowledge and Data Management, vol. 26, no. 5, pp. 1253-1266.

12. D. Chen, G. Chang, D. Sun, J. Li, J. Jia, X. Wang (2011). "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things, Computer Science and Information Systems, Vol. 8, No. 4, pp. 1207-1228.

13. I.R. Chen, J. Guo (2016). Based IoT and Its Application to Service Composition , IEEE Transactions on Service Computing.

14. I.R. Chen, J. Guo (2014). “Dynamic Hierarchical Trust management of Mobile Groups and Its Application to Misbehaving Node Detection, 28th IEEE International Conference on. Advanced Information Networking and Applications, Victoria, Canada, pp. 1-6.

15. P. Martinez-Julia, A.F. Skarmeta (2013). "Beyond the separation of identifier and locator: building an identity-based overlay network architecture for the future internet", Computer Networks, vol. 57, issue 10, pp. 2280-2300.

16. A. Jøsang, R. Ismail, C. Boyd (2007). "A survey of trust and reputation systems for online service Decision Support Systems.

17. Y.B. Saied, A. Olivereau, D. Zeghlache, M. Laurent (2013). "Trust management system design for the Internet of Things: A context-aware and multi-service approach", Computers and Security, vol. 39, pp. 351-365.

18. Y. Wang, I.R. Chen, J.H. Cho, A. Swami, K. Chan (2016). "Trust-based Service Composition and Binding with Multiple Objective Optimization in Service-Oriented Mobile Ad Hoc Networks", IEEE Transactions on Services Computing.

19. V. Sharma, R. Kumar, P. Kim (2017). “Computational offloading for efficient trust management in pervasive online social networks using osmotic computer”, IEEE Access, Vol. 5, pp. 5084-5103.

20. P. Massa, P. (2007). Proceedings of the 2007 ACM conference on Recommender systems, pp. 17-24.

21. J. A. Golbeck (2005). “computing and Appling trust in web based social network”, Doctrol.

22. Varga A, Hornig R. (2008). An overview of the OMNeT++ simulation environment[C]//Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

23. P. Deshpande, P. A. Kodeswaran, N. Banerjee, A. A. Nanavati, D. Chhabra, S. Kapoor (2015). “M4M: A model for enabling social network based sharing in the internet of things “, Int. Conf. Communication Systems and Networks (COMSNETS), pp. 1 8l.

24. J. Daubert, A. Wiesmarier, P. Kikiras (2015). “A view on private & trst in IoT”, IEEE International Conference on Communication Workshop (ICCW), pp. 2665-2670, 2015.

25. J. Duan, D. Gao, D. Yang, C. H. Chen (2017). “An energy aware trust derivation scheme with game theoretic approach in wireless sensor network for Iot application”, IEEE Internet of Things , Vol. 1, no. 1, pp. 58 69, Information sciences, 2017.

26. B. Tian, K. Liu, Y. Chen (2015). Trust and reputation model for B2C E- future internet, Vol-7, pp. 405-428.

27. Haibin Zhang (2014). “Context aware transaction trust computation in E-commerc Internet of Things Journal, IEEE, Vol-1, No-3, pp. 210-13.

28. F. Bao, I.R.chen, J. Guo (2013). Adaptive, and survivable trust management for community of internet based internet of things systems IEEE eleventh international symposium on autonomous decentralized system (ISADS), pp. 1-7.

29. L. Zhou, H. Cho (2011). “Multimedia Traffic security Architecture of the Internet of

things ", IEEE Network, Vol. 25, No. 3, pp. 35-40.

30. Y. Ruan, A. Durresi, L. Alfantoukh (2016). "Trust management framework for internet of things", IEEE international conference on advanced information networking and applications.

Corresponding Author

Shweta*

Research Scholar, Department of Computer Science, GJU, Hissar