iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** XII **Month of publication:** December 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue XII, December 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Trust Based Service in Social Networks - A Survey

Vishnu Priya.S[1], Velmurugan.M[2], Sasi Kala.D[3]
[1]Student, [2,3]Assistant Professor, Department of CSE,
Vivekanandha College of Engineering for Women, Tamilnadu, India[1]

Abstract-Internet of things is going to make a world where physical objects are unlined in corporated into information networks in order to render advanced and intelligent services for human being. Trust management plays a vital role in IOT; there is a need for robust and efficient trust management. Various security issues result in several different requirements to the design of trust management. The propose a framework to separate desired properties of trust management for each type of security issues. A Iot of service provider needs to control access to their performance and providing personalized services. This entails that the service provider requests and stores personal attributes. Nevertheless, many service providers are not sure enough about the correctness of attributes that are revealed by the user during registration. Identity management systems purpose to increase the easy to use of authentication procedures. The exhibits a new approach for user-centric identity management scheme, using trusted modules. Along with the review, we also discover some open search query for future work and accordingly present a new idea over the trust management implementation.
Keywords: Data mining, Internet of Things, Secure Computing.

I. INTRODUCTION

The Internet of things is the network of interrelated electronic sensor devices that gather data, communicate with each other, and can be supervised remotely over the internet. The goal of the IOT's development is to connect the environment and physical world to the wireless networks; this would allow making machines, objects and work environments interactive. By using IOT sensors, objects will be capable of interchanging the data with other machines without the help of human interference. The IOT includes various technology devices, infrastructure and services such as the computing, cloud computing, data analytics and mobile. The internet of things is a sensible and valid trend that is moving ahead and rapidly. There are main platforms and discoveries that have had a rich remuneration of complexity, global reach and novelty. But the IOT is for certain a trend that takes the growing of interlink to another level. There will be a mammoth range of interlinked systems and products that the IOT will enable, from elementary surveying of room temperature and security to the measure self to fully networked factories and hospitals, to automated cities. While it is genuine that the IOT will intend a major shift in the politics, economy and regulations from all government agencies, companies and non-profit organizations, here will mainly focus on the effects that it will have on citizens by arguing that, although the development of the IOT is still on early stages involving its development and spread, it is potentially a threat to both security and privacy.

Since the IOT is a growing trend, most major companies are searching to get implied, there are tremendous efforts to trigger this trend as something positive in the upcoming future. An often converse that is present in the media named the major positive technological betterment that the IOT represents. Lot of devices connected to the internet gather valuable personal data from users, such as name address, date of birth, credit card numbers and health data. The study bring out that all this data is vulnerable to potential hacker attacks. If the data that is stored in the interlinked devices stand for threat to consumer's safety and privacy, what happens when this data relies on other companies' hands is a threat as well. Insurance companies have encompass with joy the reach of the IOT, claiming that they could produce ways to collect information related to health behavior and built to design their rate oblations. Devices that calculate physical activity, blood pressure, blood sugar, weight and other health based metrics could furnish useful health information about individuals to insurance companies. The fact that the base endures the internet-connected devices is undependable and can fail exhibit a disadvantage to the IOT as well. The infrastructure that endorses the internet works otherwise across diverse geographical areas. The monopoly has the company that supply internet to users and companies. It is too expensive, undependable and it fails often. Users can spend hours or days without internet and support team is not effective and volatile. Furthermore alteration in the infrastructure and weather conditions persist as an obstacle to objects connected to the internet. In conclusion, there is the environmental wallop that the development and distribute the global IOT will bring. The Internet of things will be here sooner rather than later, for now it is a trend that is running fast to become a reality. Under this fact it is essential that we demand public access to technological knowledge about the IoT. Technology moves quicker than the development of suitable

legal valuate and action to modulate it. The IOT is something that will not damage our privacy and safety.

II. RELATED WORK

In the advance world numerous researches are going on trust based management system. Mostly the trust system falls under two category's report based and trust establishment. Here they mainly concentrating on the different schemes in the trust based management system

A. Group Based Trust Management Scheme (GTMS)

GTMS for clustered wireless sensor network, it contains a mono trust value for each and every cluster. Among every Sensor node in a cluster compute separate trust values for all group members to the cluster head. Cluster head will arrange the trust values for every single node and forwards the computed value of the base station as well as detects the mala fide node in a cluster. Based on the trust values of all the clusters, the base station assigns the one out of the three capable states, which are trusted, untrusted and uncertain to the whole group. This scheme is very easy and permissive and does not need more memory of data and difficult computations at sensor nodes. The scheme provides protection against mala field, selfish and error nodes. The prime limitation of the GTMS scheme is that use of some impractical postulates of safeguarding the trust values of clusters from attacks.

B. Trust Aware–In Network Aggregation

The trust evaluation mechanism is applied to ascertain the problematic node and identify the reliability of sensor nodes. The postulate of having always all nodes in a network working with mutual understanding and coherently with each other is not valid, when the node is changed. Normal security mechanisms can only provide a certain level of safeguarding to the network. The trust aggregation approach does not introduce extra communication overhead, which makes resources efficiently to the energy constrained in the WSNs. This approach uses multi-parent tree topology. The fragmentary aggregation results from a peculiar node will be received and processed by multiple parents. If there is any incompatibility in the result, it undergoes incompatibility checking model. Based on the result of incompatibility checking, trust of each separate node can be built up. The setup trust information can be used to identify the mala fide node in a network. Therefore, the reliability of a sensor querying is improved. The restriction of this approach is that, it suffers from the security issues of fragmentary aggregation result duplicating. Thus, it does not provide a complete security solution to WSNs.

C. Trust, Reputation System Approach

Multi criteria decision making approach is used for detecting forged aggregation result. A Gaussian probability density function is used to compute a reputation of the neighboring node based on the observed data to guarantee data authenticity and integrity. The node's opinion of the reputation is other nodes in the network. Trust is a derivation of the reputation of an entity. Total trust of a node is the compounding of communication, trust and data trust. The presented concept can be used to decide the participating nodes trustworthiness in a network

D. Trust Establishment Scheme For Cbsn

In order to monitor the behavior of every cluster node, a surveillance node is used which uses a watch dog mechanism for the evaluating trustworthiness of nodes. The trust values of the other cluster nodes stores in the node and finally the cluster head compute the trust value of each node and decide on the node revocation and select the surveillance node newly. This paper mainly contributes that it offers a cluster based trust rating model to detect the compromised sensor nodes. It develops a way to compute the trust of a cluster. The presence of no longer valid data resulting from compromised and faulty node detects by using the watchdog mechanism. Using a consensus-based outlier detection protocol in watchdog mechanism, which has a common principle of looking for consistency among the data reading. The deviation from this consensus is proportional to its level of confidence assigned to a data reading.The number of cluster nodes determined the memory of surveillance node. The cluster size depends on the number of the cluster node, the network density and the radio range of sensor nodes. This scheme is very simple and flexible and does not require complex computations.

E. Hierarchical Trust Management

This protocol can continuously change to learn from the past knowledge and adapt to change environmental conditions. This is achieved by addressing the critical design issues of trust management, namely social and QoS trust components. A novel probability

model called Stochastic Pertinent is used to characterize the assorted WSN to find the ground truth character. The paper considers a cluster based wireless sensor network consisting of cluster head and a number of sensor nodes. A sensor node reading to its cluster head through sensor nodes in the same cluster is frontward to a sensor node and then the cluster head, which then frontwards the data to the base station through another cluster head. A periodic peer to peer trust rating between sensor nodes and cluster heads is conducted by this scheme. The trust metric of two qualities of service - energy and generosity and two social trusts, namely intimacy and honesty are considered in this paper. To establish the usefulness of the hierarchical trust management protocol, In this paper, it is applied to any WSN made up of heterogeneous sensor nodes with hugely dissimilar initial energy level and dissimilar degrees of mala fide and selfish behavior's and it can use dissimilar application such as trust based intrusion detection system and trust based geographic routing . This method is more exact, but the failure of cluster head may cause to problems.

F. A Light Weight Trust Based Secure and Energy Efficient Clustering

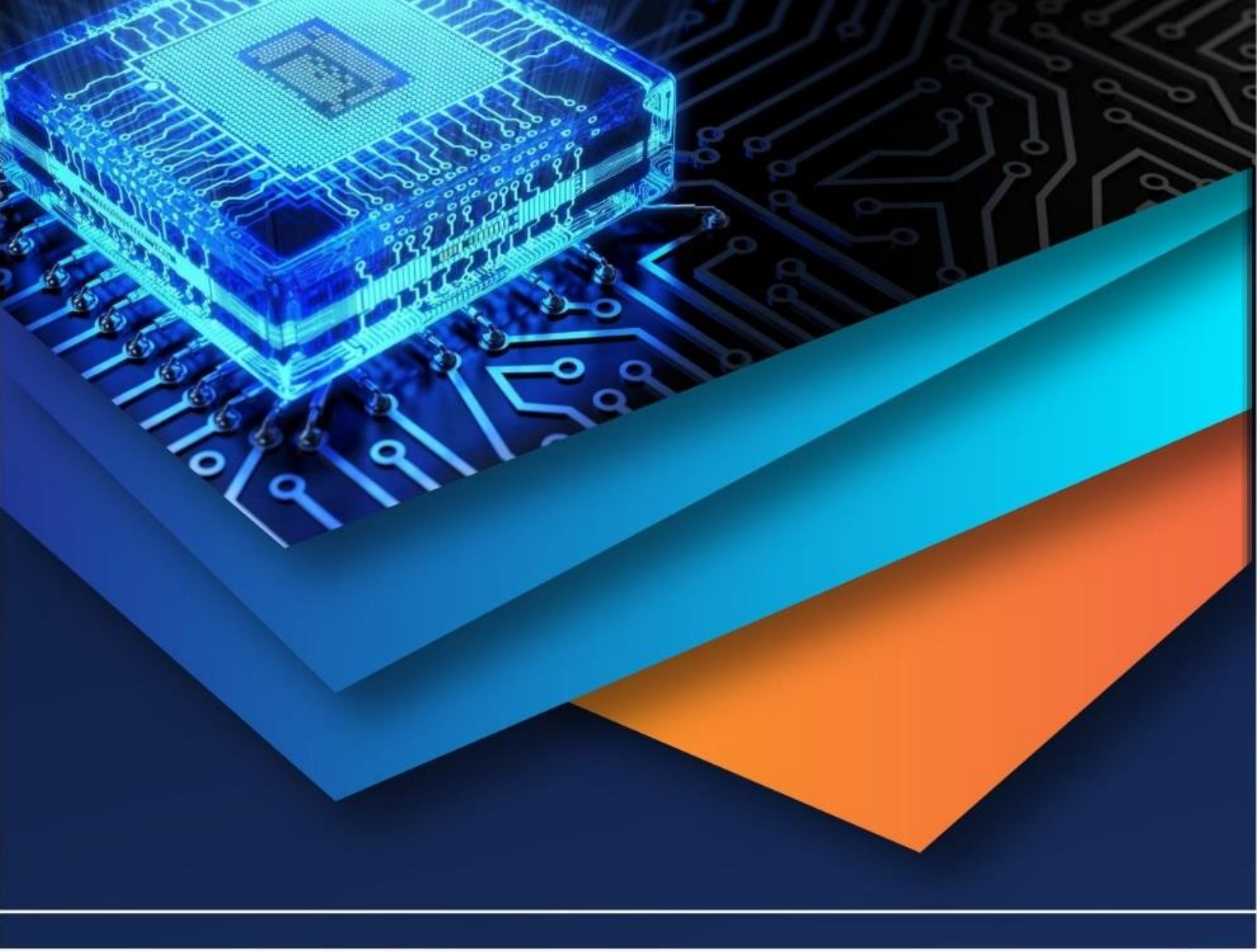
This scheme presents a trust based secure and Honey Bee Mating Algorithms (LWTC-BMA) is used by an energy competent clustering method in wireless sensor network. The proposed algorithm extends the lifetime of the network by depriving the mala fide node to become a cluster head. Data collection from multiple nodes is allowed by the clustering method to extirpate unneeded transmission, which results in energy saving. The number of nodes taking part in the communication is also reduced. The trust value of a node is computed for ensuring that the selected cluster head is not only having the maximum leftover energy, but also it has not been agreed to accept in reliability. The history of transactions with the node is evaluated from the trust value of a node and the other neighbor node gives recommendations for inside the cluster. Initially, whenever a sensor node joins the network, it is assumed that the node is trustworthy, i.e. some trust value is allocated to the node based upon the threshold trust value. This energy model is relevant for real scenarios because all the basic functionalities of a sensor node are covered.

III. CONCLUSION

The paper introduced an approach for a user-centric identity management using trusted modules. A survey on trust based management on different schemes. From those scheme is not effectively identify the user details. We proposed scheme is user-centric identity management. This scheme represents secured Internet of Things, trust model, peer to peer system which is used to interact with other peoples. Our result demonstrates the user should identify the different IDs/Pseudonyms, Credentials on Different name and distance, area. The model is capable to identify the untrusted social sites, users may have different pseudonyms with different parties and they may have different post, news, details on the sites. Finally the model demonstrated efficiency and effectiveness of the trust management protocol in IoT environments. Finally the result showed dynamic user-centric identity, trust management model could adapt to change the environments such as malicious untrusted activities.

REFERENCES

[1] Deepa S, Supriya M, "Trust Management Schemes for Intrusion Detection Systems", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106.
[2] Guangjie Hana, Jinfang Jianga LeShuc ,JianweNiud, Han-Chieh "Management and application of trust in Wireless Sensor Networks-A survey", Journal of Computer and System Sciences 2014.
[3] Z.Liu,Z.Zhang,S.Liu,Y.Ke,J.Chen ,"A trust model based on Bayes theorem in WSNs" International Conference on Wireless Communications", Networking and Mobile Computing, 2011.
[4] Y. Zhou, T. HuangW.Wang, "A trust establishment scheme for cluster based sensor networks", International Conference on Wireless Communications Networking and Mobile Computing, 2009.
[5] R. A. Shaikh, Jameel, B .J .d'Auriol, H. Lee. S .Lee, Y.J. Son, "Group-based Trust Management Scheme for Clustered Wireless Sensor Networks "IEEE Transactions on Parallel and Distributed Systems,2009.
[6] Hongmei Deng1, Guang Jin1, Kun Sun1, Roger Xu1,Margaret Lyell1, Jahn A Luk "Trust-Aware in-Network Aggregation for Wireless Sensor Networks" Intelligent Automation Inc, 2009.
[7] S. Adali et al., "Measuring Behavioral Trust in Social Networks", IEEE International Conference on Intelligence and Security Informatics, Vancouver, BC, Canada, May 2010.
[8] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, vol. 54, no. 15, Oct. 2010, pp. 2787-2805.
[9] Yenumula B. Reddy, "Trust-Based Approach In Wireless Sensor Networks Using An Agent To Each Cluster", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1, No.1, February 2012.
[10] FenyeBao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 9, NO. 2, JUNE 2012.
[11] Ing-Ray Chen, FenyeBao, Moonjeong Chang, "Trust Management for Encounter-Based Routing in Delay Tolerant Networks"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY