March - April 2020
ISSN: 0193-4120 Page No. 16959 - 16970

Holistic Trust Management Protocol for Ubiquitous and Pervasive IoT Network

Anup Patnaik[1], Banitamani Mallik[2], M.Vamsi Krishna[3]
[1]Research Scholar, Department of Computer Science and Engineering, Centurion University of Technology and Management, Odisha, India.
[2]School of Applied Sciences, Centurion University of Technology and Management, Odisha, India.
[3]Principal, Department of Computer Science and Engineering Chaitanya college of science and Technology, Madhapatnam, Kakinada.
1patnaik.a@hotmail.com, 2banita.mallik@cutm.ac.in, 3vkmangalampalli@gmail.com

Article Info
Volume 83
Page Number: 16959 - 16970
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 28 April 2020*

Abstract
Internet of things (IoT)unleashes advanced, intelligent and innovative services to human being to change their life through various application domains. Besides, IoT is new paradigm in emerging communication and information technology came to forefront in recent years draws the attention of researchers and industries to make significant contribution on different applications ranging from smart home automation, healthcare, retail, shipping, banking to smart grid. Despite its widespread presence, current researches lack in recognizing appropriate trust model which has inadequacy of addressing IoT network requirements, user concerns of security, privacy of data transmission, and also resistant of trust related attacks, therefore aforementioned pitfalls lead to notion of proposing our holistic trust management protocol in this paper to deter attacks cropping up inside ubiquitous and pervasive network of IoT fundamental infrastructure known for the characteristics of interoperability, dynamicity, and heterogeneity. In this paper we proposed dynamic trust mechanism to enhance trust between participating entities to establish communication for sharing services or resources and further, shun the attacks launched by malicious/intruder nodes only aim is to inhibit the communication inside network. Our fuzzy logic-based trust scheme approach fused into trust evaluation process of nodes and later, decision making based on degree of trust result identifies the malicious nodes. We simulated our approach considering different parameters on network simulator selecting relevant test devices and the result of which shows our proposal simulation figures out performing the existing trust models in case of detecting and isolating misbehaving nodes.
Keywords: *Dynamicity, and Heterogeneity, Fuzzy logic, Interoperability, network simulator test devices, RFID device*.

I. INTRODUCTION

Internet connectivity among physical devices, intelligent objects, convergence of multiple technologies gives birth of new ecosystem stands for anytime, anywhere, anyplace, anyone access in this ubiquitous computing world known as IoT (internet of things). Such systems demand secure and reliable message communication to support the need of heterogeneous objects interactions to achieve its goals. Further, IoT (internet of things) attained paramount attention from the research world in recent past because it can deliver indispensable quality of services which will bring up visible changes to the end users through different application domains. It's single supercomputing framework which can encapsulate all kinds of sub networks such as mobile ad hoc network, wireless sensor network, devices of RFID, actuators, sensor devices, smart devices, and cloud networking services, finally maintaining security and privacy all the participating nodes present inside its network. This complex IoT network sought after distributed trust management mechanism instead centralized scheme working through one central trusted entity consumes more energy, memory and indulged into expensive

March - April 2020
ISSN: 0193-4120 Page No. 4630 - 4637

operations to control the nodes, and limitation of its usage on applications, further even traditional approaches like access control, cryptography cannot solve network functional issues raised by nodes inside network, therefore trust management is the prime step securing IoT network and its sub networks characterized by the frequent assaults by malicious entities.

In IoT context, trust is defined with specific properties such as context sensitive, Subjective, Unidirectional, and not transitive, applicable to uncertainty environment where participants look for services through shared resources based on the degree of trust. Further, degree of trust is calculated based on the current context and nodes resource capabilities, since nodes trust level varies with the context and seeking operations which means node is offered with a service on certain trust level doesn't imply every other services would be allocated to node on the earlier evaluated trust value. We propose trust management for IoT that derives the trust value of a node considering direct interaction along with past behavior i.e. reputation obtained through requester node's presence in security groups and communities. In contrast to other trust models, our proposed scheme's indirect trust evaluation considers node value for security groups and community privilege level. Further, security groups having different privilege levels and higher security groups value stands for higher privilege level for a node so it's allowed to perform critical operations in network but same time higher community values means requester node is allowed to up take non critical write/update operations, by approaching this way clearly identifies the requester's requirement and decision for execution based on direct and indirect trust values which improves network performance. Smart objects from heterogeneous network environments are ought to cooperate with each other to achieve their common goals and communicate over wireless channel to transfer the data, now these data are completely exposed to public domain which makes vulnerable to different planned attacks by malicious, compromised and selfish nodes. Here fine tuning of indirect trust estimation included fuzzy logic approach gives new insight to our proposed trust management strategy, also makes more robust and unique than other models to stand before functional requirements of IoT network. Instead of implanting centralized trust management sever to handle trust load calculation, which is very expensive business for application scenarios, therefore the better sense would be to realize the need of distributed trust management technique but must deliver following multi-fold advantages to be adopted across IoT applications

- Light trust mechanism fit to different types of objects functional requirement in heterogeneous environment
- Identification of abnormalities related to nodes behaviour
- Reduce communication overhead finding trustworthiness of adjacent nodes
- Reduce computation overhead to prevent depleting nodes power & memory
- Able to address aspects of interoperability, dynamicity, and heterogeneity of IoT architecture
- Resistant to trust related attacks such as bad mouthing, on-off attack, and selective attack

Main crux behind design and implementation of any trust security protocol is to address the issues of authentication, authorization, access control, service data transmission control, and identity management, that the nodes are facing in the network. In literature survey further sections, there are other means to tag the node as trustworthy but most viable and efficient solution at present to do analysis on past behaviour of nodes i.e. reputation/recommendation derived from past interactions and consider present activity that trustee supposed to do, combination of present and past components as cited above plunges the nodes with the intention to perform unwanted activity.

March - April 2020
ISSN: 0193-4120 Page No. 16959 - 16970

Keeping the hope to have efficient management system, our trust management solution pertains to distributed management mechanism for trust evaluation and assessment having below contribution to the solution

- ❖ Establish efficient distributed trust management strategy to support different type of sub networks protocols residing inside IoT
- ❖ Able to address inherent attacks inside network
- ❖ Light weight trust management scheme using fuzzy based approach
- ❖ Reduce incurring communication and resource usage overheads while securing the network
- ❖ Direct trust and reputations of security groups, communities considered
- ❖ Draws simulation analysis on factors influencing decision making process
- ❖ Conclusion with current model bottlenecks and suggestion for improvising

Finally, the reminder of the paper is organized as below, section 2 will focus on current state of art trust management practices for IoT, also highlights key shortcomings on existing mechanisms which enables us to establish new proposed protocol in the future section. Section 3discusses about design of our proposed trust management model and Section 5 outlines the analysis on the simulation results followed by summary and direction of new research in Section 6 conclusion.

II. LITERATURE REVIEW

Chakravartula and Lakshmi [1] proposed HEXAGON model for trust management framework using six key factors to compute the trust for IOT based medical devices. It used the fuzzy logic to find the trust value with help of interference engine part of Trust Management Framework and Communication across the peers for calculating TV is completely secured through pre-shared key of cryptographic API. Main issue with this model, it's not tested with real time application and finding reputation of device may not get correct value as it considers only concern of service provider. Alshehri and Hussain[2] fuzzy logic based approach is able to identify the attacks such as on-off attacks, contradictory behaviour attacks, bad service provisioning attacks, caused by malicious nodes and also established message communication which enables secure communication of messages among the nodes while computing the trust value. Further, this approach suits to the cluster-based trust management in IoT. Efficiency of this approach may not be achieved if scalability and long period of simulation are considered to perform.

Khan and Herrmann [3] trust management technique Subjective Logic building Intrusion Detection Systems (IDS) are suitable for resource constraint tiny devices to protect from malicious attacks. This approach helps to find various network-based attacks to IOT and single out the malicious nodes from network. This mechanism considers direct trust and also maintains three algorithms i.e. centralized and distributed to manage reputation of neighbour nodes. Best part of this approach is it generates lesser number of false positives and prevent redundant packet transmission for detection of intruder nodes. Wu and Li [4] provided trust model for multi domain RFID system includes diversity of trust evaluation without reputation i.e. past interaction of readers. Multi domain RFID means trust evaluation from intra-domain, inter-domain and cross domain between tags and readers. Here Hierarchical trust management framework approach is having two layers which are RFID reader trust layer base on D-S evidence theory-based scheme (D-S scheme) and verification of interaction proof based scheme (VIP scheme) and authentication center trust layer based on administration center working as centralized way. This multi domain trust model is not used against different threats to system and its performance also not measured.

Abhijit and Prasad [5] proposed application layer trust-based security model for IoT and fog

March - April 2020
ISSN: 0193-4120 Page No. 4630 - 4637

computing based application. This model focuses on application layer of IoT is suitable for the applications where the sensitive data must be collected from IoT devices and security of data is also important for analysis, mainly healthcare domain.Suryani et al. [6] uses both current trust assessment and objects past experience known as reputation value are included finding the trust values. For reputation, instead depending on historical data, it uses time parameter to get correct value of reputation without much variation. In this model, all the objects are filtered through the Diffie-hellman authentication, hence no new objects out of this authentication process can send fake trust and reputation value. Security models using this trust assessment are yet to developed to address trust-based attacks.

In this model, all the objects are filtered through the Diffie-hellman authentication; hence no new objects out of this authentication process can send fake trust and reputation value. Security models using this trust assessment are yet to developed to address trust-based attacks. Nabil et al. [7] discussed number of different trust models based on the different contexts and also presented comparative study of trust-based approaches according to the models. Ideally trust model should establish trust of entities in each layer, then privacy, key management, trust routing and quality of services (QIoTs).Khan [8] realized vital role of secured IoT devices for smart cities in highly resource constrained environment with the property of low processing power and battery replacement not feasible for devices, so in this need of hour, Expecting lightweight mechanism which can provide security solution in smart city environment to let devices consume less energy and also detects malicious behaviour of nodes efficiently. There are three trust-based algorithms were proposed, and appropriate one is selected based on threats, and energy consumption.

Bao and Chen [9] recognizes great challenge into security and reliability management after device being connected in heterogeneous network environments. Its scalable trust management protocol considering trust properties honesty, cooperativeness, and community-interest to evaluate trust. It tried this protocol only for service composition application, not for other trust based IoT applications in presence of malicious node activities. Caminha et al. [10] proposed smart trust management based on machine learning and an elastic slide window technique to identify on-off attacks and fault nodes. This approach also helps to differentiate broken or temporary malfunctioning nodes and misbehaving devices in the IoT network. Both in simulated environment and real time scenario, it maintains good precision level of finding OA attacks.In future, this model elastic sliding window concept can be extended to trace other trust related attacks, which so many other models are able to find.

Alshehri et al. [11] DTM-IoT provides trustworthy communication among the devices in IoT network using Cluster Node (CN), Master Node (MN) and a Super Node (SN). This model with structural change can be applicable to both centralized and distributed trust management system. This approach is not verified against trust-based attacks and how it will behave in resource constrained IoT application. In this model the whole network is divided number of clusters based on the trust values, node can request the master node (MN) to join to its cluster or asking redirect to another cluster. Super node on the top handles the nodes to join clusters with similar trust value, also additional communication of cluster nodes and master nodes. Kowshalya and Valamathi [12] facilitates trust management scheme based on object behavior in Social Internet of Things (SIoT). This approach uses trust metrics namely direct trust, indirect trust, centrality, community Interest, cooperativeness, service score to compute trust among objects. This model considers other trust metrics other than direct and reputation values to make reliable IoT network. Two nodes can find the trust between them directly

March - April 2020
ISSN: 0193-4120 Page No. 16959 - 16970

or through intermediate nodes. The advantage of employing this model is it isolated bad nodes from network, so allowing to perform its task for low trust value network.

Patil and Bhonsle [13], SIoT could bring the security in connecting heterogeneous devices through social relationship as trust to share resources. It outlines three-layer architecture for the increasing connectivity and improving availability in SIoT containing man components SIoT server, the Gateway and the objects. The simulated result obtained through the finite automata shows minimum path length assigned between randomly selected nodes in SIoT than a random network. Yet this model has to be tried with real time applications. The Arabsorkhi and Haghighi [14] conceptual model is capable of handling node in dynamic and decentralized networks, and its algorithm very much like the approach of humans following in daily social life. Service seeker node could be able to find the provider as trusted/not based on the responders' feedback. This conceptual model parameters can be calibrated to satisfy the needs of many other IoT applications depending on the trust level. The model is yet to be analysed on real large-scale graph by means of simulation. It involves four trust modelling processes starting information gathering to final provider selection then update the database based on the transaction experience.

Alshehri and Hussain [15] delivers centralized trust management mechanism where trust module will act as main component of central trust manager. Super node keeps trust module and other modules as part of trust management framework to provide trustworthy communication between all nodes. In this approach Super node plays centralized trust manager node having central repository of the trust management system. Whole IoT environment is divided into different clusters, each cluster having one master node and many cluster nodes. Maser node is termed as local repository to store trust values of cluster nodes, and SN will keep all trust data of MN and CN. Lize et al. [16] proposed trust-based control mechanism based on architecture modeling of IoT. Trust mechanism is implemented each layer of network, finally decision is made by service requester based on collected trust information and requester policy. Through the trust management, it's able to create self-organized network after finding the best partners in and around of service requester. This trust mechanism and decision-making approach can be used to assist other compatible security mechanism for finding untrusted (trusted) entities based on node trust value. More important step in the trust framework is decision making based on trust, firstly its related to access control policy where user's identity authentication and privacy protection are measured and then secondly distributed trust control policy, actual service is provided to the user.

Saied et al [17] avoids adding all the past experiences into single metric to calculate the global trust, instead its context aware and multi-service trust management system doesn't hide heterogeneity of IoT nodes like existing trust models, considers current context and resource capabilities suitable to new requirement of IoT. This approach five phases trust model not only gives priority to critical services for provision but also prevents happening of bad mouthing, on-off selective forwarding underlying attacks inside network. Alshehri et al. [18] identified real issues in IoT security in presence of large number of devices, mainly cause of concern is the bad mouthing of trust values makes the node unsuitable to practical IoT applications. Here proposed model is scalable trust management solution in the IoT able to address pressing and practical issues related to trust based IoT trust management having the integration of four algorithm, 1.Preventing bad mouthing of trust value, only considering real values, 2. intelligent trust-based formation of clusters, 3. trust based migration and 4. Cluster nodes state based on trust values.

March - April 2020
ISSN: 0193-4120 Page No. 4630 - 4637

Wang et al [19] established trust-based framework for layered IoT which is decomposed into Sensor, core and application layer. Its functionality based on three source of information such as service, decision-making and self-organizing of series of nodes to perform tasks like package forwarding and sensing of data in network scene. Yet to build the trust model & integrate into this general trust management framework.

Khan et al. [20] proposed trust-based routing solution for Low power and lossy networks. This TRPL is lightweight mechanism to detect and isolate the bad nodes from network resulting in better network performance than other RPLs. These different variant of RPLs suffer from false positives but TRPL among formers displays fairly low rate. TRPL involves steps of trust evaluator, trust value combination and further, establishment of trust result. In Evaluation step, it considers belief, disbelief and uncertainty factors where all three results to 1 value and in next step, combination step, it uses subjective logic to combine the trust value of a node received from the neighboring nodes, finally in last step, DODAG graph is reconstructed based on the trust result, nodes with less than threshold level are removed from the graph.

Through the above state of art, it's very much clear in IoT with different type of devices associated with multiple applications and varied network communication protocols need a holistic trust management solution to have trustworthy transactions inside network. Our proposed solution looking at research arena downsides for security & privacy of network has come up a lightweight holistic trust management protocol considers direct/indirect interactions along with other parameters strongly relevant to model.

III. HOLISTIC TRUST MANAGEMENT PROTOCOL

To make every interaction between provider and requester trustworthy, then our proposed model in IoT network identified mutually exclusive independent below steps, no other models in state-of-art considered pre-state of nodes before operations, which is part of Node Capability step in this model Fig.1.

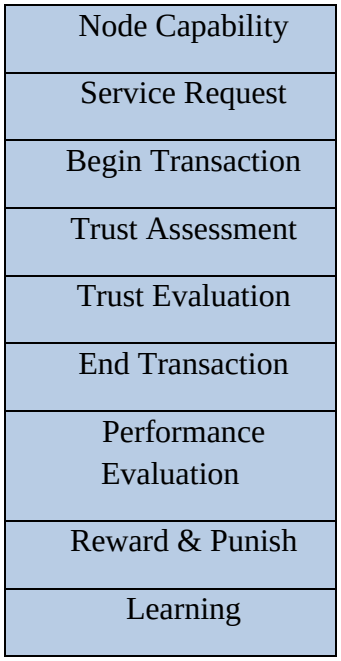

Figure 1. Proposed Trust Model Steps

- Node Capability

  Here it considers requester ability to complete the operation, it shouldn't happen such that requester leaves operation in the middle, it may happen due to multifold reasons as depleting of residual energy, memory exhaust, mobility of node, and bandwidth. If pre-assessment of provider node is done before requesting for the operation, then

- Service Request

  Device will request for relevant service or resources to fulfill its goals, either goal or part of goals objective will be interpreted as service request.

- Begin Transaction

March - April 2020
ISSN: 0193-4120 Page No. 16959 - 16970

When Previous step is initiated then transaction will be started. Every transaction is defined service request's purpose and accomplishment.

- Trust Assessment

  Before providing requested service by provider, it begins process of finding details of requesters trustworthiness through different parameters defined in our trust model.

- Trust Evaluation

  Based on the collected parameters in the above step, now it's the prime step to evaluate the trust metrics which decides to render the service or not to the requester.

- End Transaction

  Transaction is terminated with acknowledgement to requester, if provider is showing interest to allocate or not, this decision is taken based on the trust metrics value and application threshold trust value.

- Performance Evaluation

  System as whole can be improved based on experience gained by provider and requester. Analysis on performance build up new concepts to protect security and privacy of nodes.

- Reward & Punish

  This step is applicable to both provider and requester.
  If any failure on the transaction side after assigning service, then fine to requester.
  If fail to provide service after well trust value, then fine to the provider.

- Learning

  This step is applicable to both parties which are involved in the transaction processing and also this result brings changes in trust model handling complex critical application.

Proposed trust model with above steps framed the trust metrics to evaluate the trust of the operation which involves provider, requester and intermediate nodes, no other algorithms focused on trust of operation, all contemporary algorithms focused either evaluate requester or provider trust.

Trust Metrics is defined as bellow

$$TV^{(Y)}By^{(X)} = a\ SSG(Y) + b\ CEB(Y) + c\ CG(Y) + d\ DI(Y) + e\ ACP(Y) + f\ PRII(Y)\ldots (1)$$

- $TV^{(Y)}By^{(X)}$: Trust value of Y evaluated by X, Y: Service Requester and X: Service Provider

- a, b, c, d, e, and f are constants and their values are floating between 0 to 1 depending on varied network size and complexity of IoT applications.

- SSG(Y): Subscribed Security Groups of Y, based on the type of security groups Y has such type of privilege to request. If any device joins the network, without any verification starts communicating to other nodes, then certainly initiated operation is prone to attacks. In this model, service requester device should be part of security groups before any operation, that will compel the node to share credentials to be part of groups, this premeasured step will prevent many nodes, which just joined in network to spread uncertainty in the network sending false reputation, capturing sensitive data, drop data and ignoring acknowledgements.

- CEB(Y): Common Elite Buddies of X about Y

  All other contemporary algorithms send request to all neighbor nodes to get status of node requester saying that is there any chance of neighbor nodes interacted with Y before and if Yes, send acknowledgement back to provider. In our model, instead spending more time reach out to our neighbors, only focus on elite buddies of X, through this approach not

March - April 2020
ISSN: 0193-4120 Page No. 4630 - 4637

only saves time but also makes information reliable.

Algorithm 1: Find the common elite buddies list of X, CEB(X)

Input: X and CEB(X) List, is empty in the beginning

Output: Generate CEB(X)

1. Y sends request to X to get the service
2. X calculates trust metrics of Y as per above equation 1
3. If $Trust_{Cal} > Trust_{Thres}$
   Assign service to the Service Requester
   Else
   Deny Service to the Service Requester
4. In Reward & Punish and Leaning Phase, its analysed if Y fulfilled its goal after getting service and no trust related attack during the transaction
   Add Y to CEB(X) List
   Else
   Ignore Y, no add to CEB(X) list

- CG(Y): Community Group component focuses on the devices which start communicating with other providers based common interest. Probability of getting reputation of device through minimum spanning of request and easier to understand requester requirement are the advantages stays with this proposed model, so IoT networks need not to be a SIoT to find the trust belonging to the same community group.

- DI(Y): Direct Interaction X to Y

  To get trust value of direct interaction of X to Y if happened before, if not in our model Use of CEB or CG concepts will help to get the trust value of interactions with Y through intermediate nodes.

- ACP(XY): Additional Check Points of X and Y, few other parameters are considered before initiating operation.

  - Both parties should be in sync for bandwidth frequency, otherwise getting trouble for sending and receiving service request.

  - Residual battery powder of Y to process the service after granted.

  - Local memory of Requester to store Data

  Our trust model assumes that Providers in general are rich in resources, battery power, memory and other resources, therefore not considering any checkpoints for Provider while calculating trust metric.

- PRII(Y): Prioritized Reputation Indirect Interaction X to Y This step is to receive reputation of Y in IoT network, just like to know persons reputation in social life, device reputation builds up in period, not immediate span of time. In our trust model, this reputation value (Y) follows transitive property can be obtained through X CEB or X CG nodes.

Algorithm 2: Find the Reputation of Y, PRII(Y)

Input: X and CEB(X)

Output: Reputation Value of Service Requester

1. X sends request to its own common elite buddies, instead sending to all neighbourhood nodes
2. CEB nodes further sends the same request to its subsequent sub CEB nodes to find whereabout of Y, this searching process will continue in recursive way till Y is found.
   Var iNodes = CEB(X);
   int iStep = 1;
   curReputation = 0;

March - April 2020
ISSN: 0193-4120 Page No. 16959 - 16970

```
FindReputation(Nodes iNodes, int iStep)
{
 Node temp = Popup(iNodes);
 If (temp ==Y && iStep <= n)
    {
     Remove (temp from iNodes);
    temp = Popup(iNodes);
      Return (curReputation += Reputation (Y))
    }
    Else if (iStep <= n)
     Find Reputat in(CEB(temp), iStep++);
    Else if (iStep > n or is Empty(iNodes))
    Return;
}
```

3. Once Y is found, bottom nodes communication will traverse back to X to intimate reputation value.
4. Now X accumulates all the received reputations of Y through different intermediate nodes who had prior experience working with Y.
5. X selects the reputation of Y based on age and duration of interactions, it means priority is given to those reputation which obtained from latest and long-time duration interactions, in this approach our trust model can avoid bad mouthing attacks.

Proposed trust model workflow is explained in below steps of Fig2.

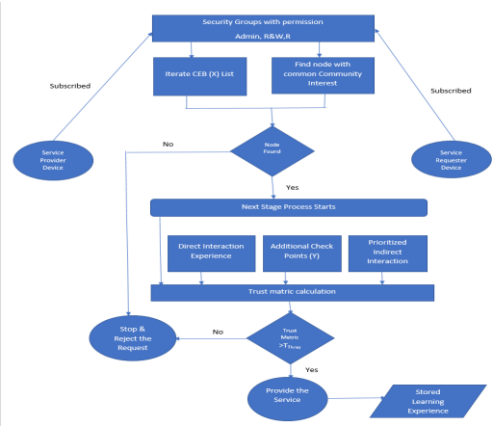

Figure 2. Proposed Trust Model flow

IV. RESULT AND DISCUSSION

Our proposed model is simulated against network simulator with wireless nodes and gateways as mentioned in the Table-1. From the experiment, it clearly shows our proposed model stands tall against the malicious nodes which are initiating bad mouthing, selective forwarding attacks. Nevertheless, the IoT system is vulnerable to both malicious and malfunctioning activities, considering the additional checkpoints of service requester and provider in trust matric equation, our proposed model can also prevent the malfunctioning of nodes, no other existing algorithms can do so with their respective approaches. Our proposed model network topology includes WPAN (Wireless Personal Area Network) using protocol like Zigbee (IEEE 802.15.4), 6LowPAN and also having WLAN (Wireless Local Area Network) protocol Wi-Fi (IEEE 802.11a) is to be used.

Table-1: Simulated against network simulator with wireless nodes and gateways as mentioned

Parameter	Value
Number of Nodes	100
Number of Clusters	10
Simulation Time	45
Simulation Area	60×60
Initial quality of recommendation	1
Services	6
Malicious assisting nodes	10%

March - April 2020
ISSN: 0193-4120 Page No. 4630 - 4637

Our approach compared with the centralized trust mechanism Alshehri and Hussain [15], then simulation figures show that our proposed model outperforms the existing centralized trust algorithm w.r.to time and transactions in Fig.3 and Fig.4. Trust level increases gradually with time because received accurate reputation values, considering additional checkpoints of device such as memory and battery power to transmit the data, subscribed security group privileges., in case of centralized model its always difficult to handle critical application, very specific to particular scenarios only. Overburden on centralized nodes involving trust level calculation seems very much unwary preventing malicious nodes.

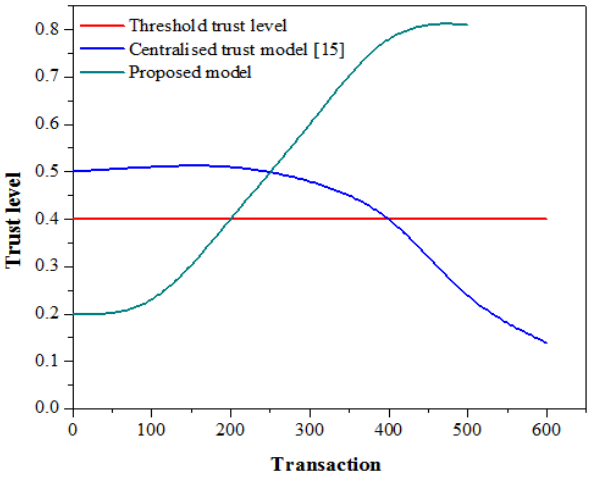

Figure 3. Trust Level vs. Transactions

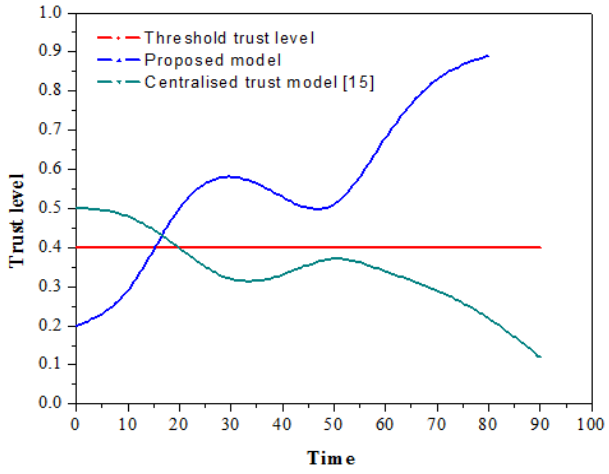

Figure 4. Trust Level Vs. Time

V. CONCLUSION

Our trust-based service model outperforms contemporary trust and non-trust-based models handling privacy and security in IoT network. Yet, this proposed model could be tried for real time very complex application with short range, tiny devices, NFC devices with heterogeneous IoT network. Next proposed model, instead of keeping devices on varied network positions, nodes can form cluster node groups based on node trust vector value, and the cluster head will be having highest trust value among all the nodes in that group, secondly if node falls below threshold trust level, there is scope of migration of specific node from one cluster to other cluster, in such ways the proposed model can keep critical applications handling nodes in high trust zone ,followed by keeping Medium, Low trust zones based the service requirement.

REFERENCES

[1] Raghu Nallani Chakravartula1 and V. Naga Lakshmi 2017. Trust Management Framework for IoT based P2P Objects //International Journal of Peer to Peer Networks (IJP2P).-2017.- No 8(2/3).-p.17-24

[2] Mohammad Dahman Alshehri, Farookh Khadeer Hussain 2019. A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)// Computing.-2019.- No 101(7).-p.791–818

[3] Zeeshan Ali Khan, Peter Herrmann 2017. A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things // IEEE 31st International Conference on Advanced Information Networking and Applications (AINA). DOI: 10.1109/AINA.2017.161

[4] Xu Wu, Feng Li 2017. A multi-domain trust management model for supporting RFID applications of IoT // PLoS ONE 12(7): e0181124. doi.org/10.1371/journal. pone.0181124

[5] PatilAbhijit J, G. Syam Prasad 2018. Trust Based Security Model for IoT and Fog based Applications // International Journal of Engineering & Technology.-2018.- No 7(2.7).-p.691-695

March - April 2020
ISSN: 0193-4120 Page No. 16959 - 16970

[6] Vera Suryani, Selo Sulistyo, Widyawan Widyawan 2017. ConTrust: A Trust Model to Enhance the Privacy in Internet of Things // International Journal of Intelligent Engineering and Systems.-2017.- No 10(3).-p.30-37

[7] Djedjig Nabil, D. Tandjaoui, Imed Romdhani, Faiza Medjek 2018. Trust Management in Internet of Things, Trust Management in Internet of Things. Security and Privacy in Smart Sensor Networks // Edition: 1st Edition, Publisher: IGI Global, Editors: Yassine Maleh, Abdellah Ezzati, Mustapha Belaissaoui. DOI: 10.4018/978-1-5225-5736-4.ch007

[8] Zeeshan AliKhan 2018. Using energy-efficient trust management to protect IoT networks for smart cities // Sustainable Cities and Society.-2018.- No 40.-p.1-15

[9] Fenye Bao, Ing-Ray Chen 2012. Trust management for the internet of things and its application to service composition // IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM) **DOI:** 10.1109/WoWMoM.2012.6263792

[10] Jean Caminha, Angelo Perkusich, Mirko Perkusich 2018. A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things // Security and Communication Networks. doi.org/10.1155/2018/6063456

[11] Mohammad Dahman Alshehri, Farookh Hussain, Mahmoud Elkhodr, Belal Saeed Alsinglawi 2019. A Distributed Trust Management Model for the Internet of Things (DTM-IoT) // Recent Trends and Advances in Wireless and IoT-enabled Networks. doi.org/10.1007/978-3-319-99966-1_1

[12] A. Meena Kowshalya, M. L. Valarmathi 2017. Trust Management in the Social Internet of Things // Wireless Personal Communications: An International Journal.-2017.- No 96(2).-p.2681-2691

[13] Preeti Patil, Mansi Bhonsle 2016. Trust Management in Social Internet of Thing // IJCA Proceedings on National Conference on Advances in Computing, Communication and Networking ACCNET.- 2016.- No (5).-p.14-17.

[14] Abouzar Arabsorkhi, Mohammad Sayad Haghighi, Roghayeh Ghorbanloo 2016.A Conceptual Trust Model for the Internet of Things Interactions // 2016 8th International Symposium on Telecommunications (IST'2016), Tehran, Iran

[15] Alshehri M.D., Hussain F.K 2018. A Centralized Trust Management Mechanism for the Internet of Things (CTM-IoT). In: Barolli L., Xhafa F., Conesa J. (eds) Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2017. Lecture Notes on Data Engineering and Communications Technologies, vol 12. Springer, Cham

[16] Lize Gu, Jingpei Wang, Bin Sun 2014. Trust management mechanism for Internet of Things // China Communications.-2017.- No 11(2).-p.148 - 156

[17] Yosra Ben Saied, Alexis Olivereau, Djamal Zeghlache, Maryline Laurent 2013. Trust management system design for the Internet of Things: A context-aware and multi-service approach // Computers & Security.-2013.- No 39.-p.351–365

[18] Mohammad Alshehri, Farookh Khadeer Hussain, Omar Khadeer Hussain 2018. Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT) // Mobile Networks and Applications.-2018.- No 23(3).-p. 419–43

[19] Jingpei Wang, Sun Bin, Yang Yu1, Niu Xinxin 2013. Distributed Trust Management Mechanism for the Internet of Things // Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013), Atlantis Press, Paris, France

[20] Zeeshan Ali Khan, Johanna Ullrich, Artemios G. Voyiatzis, and Peter Herrmann 2017. A Trust-based Resilient Routing Mechanism for the Internet of Things // In Proceedings of ARES '17, Reggio Calabria, Italy, August 29- September 01, 2017

AUTHORS PROFILE

Anup Patnaik*, Research Scholar, Department of Computer Science and Engineering, Centurion University of Technology and Management, Odisha, India. Email: patnaik.a@hotmail.com

Dr. Banitamani Mallik, School of Applied Sciences, Centurion University of Technology and

March - April 2020
ISSN: 0193-4120 Page No. 4630 - 4637

Management, Odisha, India Email: banita.mallik@cutm.ac.in

Dr. M.Vamsi Krishna, Principal, Department of Computer Science and Engineering Chaitanya college of science and Technology, Madhapatnam, Kakinada, Email: vkmangalampalli@gmail.com