International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5826
***Article Received**: 24 September 2022 **Revised**: 31 October 2022 **Accepted**: 10 November 2022*

Study of Trust Aggregation Authentication Protocol

Meena Gulati[1], Dr. Rakesh Kumar Yadav[2], Dr. Gaurav Tewari[*]
[1]Research Scholar, Department of Computer Science Engineering,
Maharishi University of Information Technology, Lucknow
[2]Research Supervisor, Department of Computer Science Engineering,
Maharishi University of Information Technology, Lucknow
[3]Faculty, School of Information and Communication Technology,
Gautam Buddha University, Gr. Noida.[*]

Abstract— The main focus of this work is to sense and share the data that are required to be trusted and the solutions are to be provided to the data, as trust management models. Additionally, the elements in the IoT network model are required to communicate with the trusted links, hence the identity services and authorization model are to be defined to develop the trust between the different entities or elements to exchange data in a reliable manner. Moreover, data and the services are to be accessed from the trusted elements, where the access control measures are also to be clearly defined. While considering the whole trust management model, identification, authentication, authorization and access control are to be clearly defined.

Keywords- IOT, TRUST MODEL, BVT, DVT, MAC

I. INTRODUCTION

In the present scenario of human lives, Internet of Things (IoT) impacts in greater ways the various domains. Moreover, the IoT model defines a protocol for framing the efficient usage of IoT applications. Hence, security and trust management models play a vital role in IoT for securing data and devices from attacks. The heterogeneity of IoT elements, nature of the communication links and other IoT features lead it to many security problems in each layer of IoT. Those vulnerabilities are to be managed and handled effectively; hence the other elements in the IoT environment are to be secured. Likewise, uncertainty and the effectiveness are the key factors of IoT model deployments, where the elements could be insecure and attacked. Therefore, trust management is very important in the IoT model for providing reliability, user privacy and data security.

II TRUST MANAGEMENT MODEL BASED ON IOT LAYERS

The IoT layers are open or vulnerable to various attacks and threats. Since, designing trust management for IoT layers are complicated, the trust mechanism is defined for each layer. Trust management model is the model to guarantee the trustworthiness of the service providers of the cloud model, since it provides various access levels to Service Level Agreement (SLA), security, performance and so on. The model defines solutions based on, i. Self-organization of sensors, ii. Secure Routing, iii. Message Control in Network Layer and iv. Multiple Services.And, the pictorial representation is shown in figure 1, for the trust management in iot. The application layer is the main layer, considered here for security.

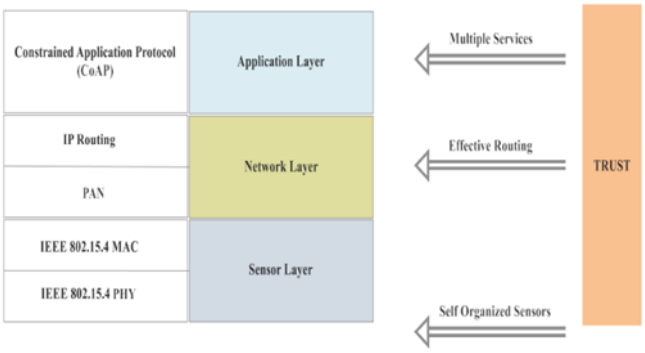

Figure 1 Trust based iot layers

DATA AND BEHAVIOR TRUSTS FOR TRUST MANAGEMENT IN IOT

The Trust Management Model provides standard for security policy specification and attribute of security policies. The model defines the implementation of data security and access control process. Figure 2 denotes the general flow of trust management model that uses the trust data for providing secure communication between the cloud users and providers. Here, evaluation of user behaviours is carried out for both the users and providers of cloud resources, based on the recent user activities, and their abnormal behaviours. And, the data trust is measured based on security, privacy and accountability, which are significant for providing cloud data security with the trust management design.The Behavior Trust Rate can be evaluated based on the following factors,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5826
***Article Received**: 24 September 2022 **Revised**: 31 October 2022 **Accepted**: 10 November 2022*

1. Frequency of direct communication between sensors
2. Time slot of each communication
3. Amount of positive communication between entities
4. Amount of negative communication between entities
5. Amount of tentative communication between entities

Moreover, data trust rate is evaluated based on the deviation of each entity on their prompt information. But, the evaluations have some time and computational complexities. In general, there are three major attacks such as,

a) Self-Promoting
b) Bad-Mouthing
c) Ballot Stuffing

Since, the communication performs operations such as, packet forwarding, exchange of communication data, Medium Access Control (MAC) layer data communication and so on; the models are open to various attacks. Furthermore, for solving the problems in trust based evaluations, the trust rates are computed with respect to each cluster head for effectively detecting the attacks. Additionally, the computations are carried out based on direct and indirect remarks. And, the trust rate is computed based on the communication between the IoT devices. The distance between the server and the element is derived for trust rate. The behaviour trust is derived based on the direct communication between devices. The entities that forward the trust rate of each node to their central node are to be secured and trusted.

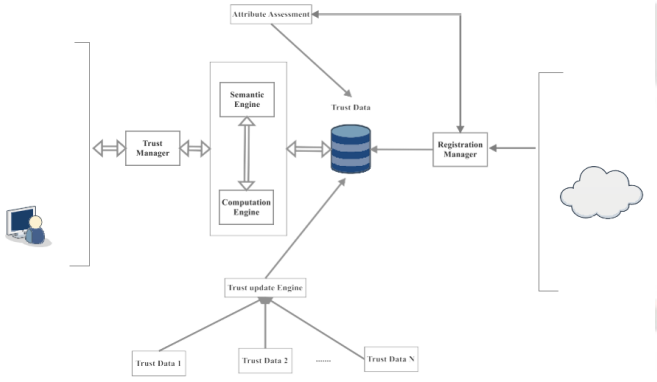

Figure: 2 General Flow of Trust Management Model

Basically, the system model consists of sensor nodes, gateways, and a server. In the system architecture, mutual authentication should be provided between the devices and also between the device and the gateway. The diagrammatic representation of the system architecture is presented in figure

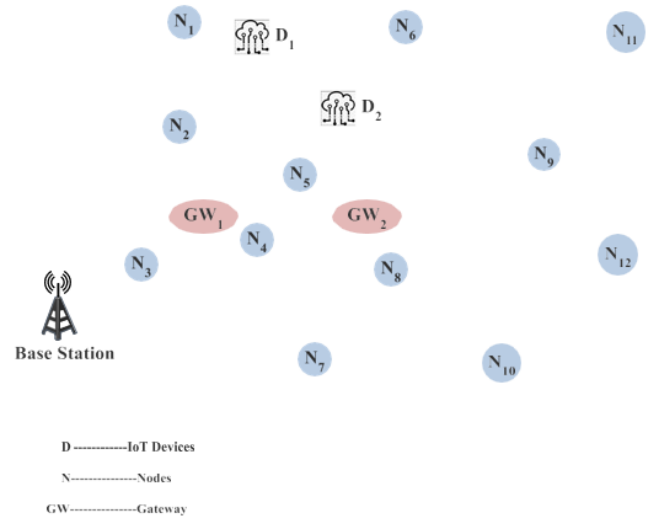

Figure 3 System Architecture of TAAPML

The BTV for each device is computed based on the successful rate of route request and successful rate of packet delivery and rate of data forwarding.

Computations of BTV and DTV

The Behavioral Trust Value (BTV) is computed by the equation 1,

$$BTVi = SRRR + SRRP + DFRi + PDRi \quad (1)$$

Authentication between Devices

The authentication between the IoT devices is processed by checking the identity and the validity of the devices involved in the communications. And, the operations are explained with the following steps.

1. Each node Na transmits the Hello message to their adjacent devices, which comprises of the node identity, sequence number, $SRRR$, $SRRP$, $DFRi$ *and* $PDRi$. And, the format of the Hello message is shown in figure 4.
2. The reply message is transmitted from the adjacent node to the source node with complete data about them.
3. Using the data BTV is computed and transmitted to gateway
4. Data Aggregation is carried out in gateway and the collective BTV of each node is derived as given in equation 2,

$$BTVCi = \sum BTVi(t) \quad (2)$$

5. The gateway computes the DTV using the formula in equation 3 Total Trust Value (TTV) is derived as in equation 3

$$TTVi = BTVCi + DTVi \,(3)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5826
***Article Received**: 24 September 2022 **Revised**: 31 October 2022 **Accepted**: 10 November 2022*

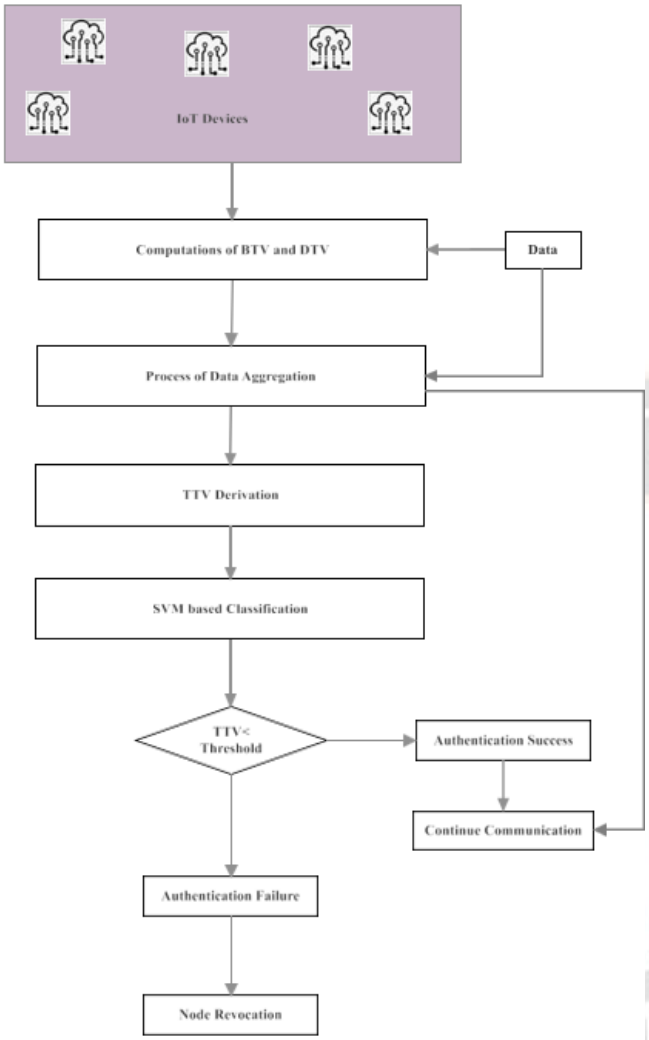

Figure 5 Operations in TAAPML

Authentication between Device and Gateway

When the data is received at the gateway point, the TTV is verified, and, when it is lesser than the threshold value, then the node is revoked from communication.

1. The threshold TTV is computed using SVM classification.
2. When the TTV is greater than the threshold, authentication is provided.
3. The secret keys are transmitted to the nodes from the trusted authority using the Authentication Token ATi, which is calculated as in equation 11,
4. $ATi = HMAC(IDi \oplus (\alpha, \gamma))$ (11) Where, 'IDi' is the node identity, α, γ are the randomly selected prime numbers.
5. Operations performed for Ensuring Data Confidentiality

This section presents the operations performed for data confidentiality in the devices and the gateway points. And, the steps involved for data confidentiality are discussed in the following section. Here, data confidentiality is computed for device end and gateway point. In gateway, the HMAC is derived based on the device identity, message and user data. Following, the trust values are computed based on performing XOR with authentication token.

Initially random number was taken and named as "$r1$" and "$r2$". The total trust value is calculated based on the cumulative value of behavioural and data trust value. The Hash key generation is calculated based on the XOR operation between Authentication token and random number "$r1$". Then the Hash key value along with

TTV performs the logical operation with random number "$r2$" and calculates the value of "X". Hash function of total trust value concatenated with node identity performs XOR operation with hash function of authentication token that gives M1. Later, the Hash-based Message Authentication Code is derived with node identity, Hash value of message (X), M1, random number ($r1$), and mb.

Incorporation of SVM for Attack Detection

Support Vector Machine (SVM) is the classification technique used for training the model with the authentication factors of legitimate device factors. Since, this classification model is very appropriate in performing binary classification, the testing phase involves in classifying the data under two class sets as, authenticated devices and others. The steps of TTV trusted rate is given in table 1.

Table 1 Pseudo Code for calculation of TTV Threshold

1. Begin
2. Collect Traffic Flow from IoT devices
3. Frame feature set as, X_{ab}
4. Frame the training set as (X_{ab}, Y_{ab})
5. For each input $F_i \forall$ device
6. Do
7. Remove data from F_i
8. Compute the average TTV
9. End Do
10. Compute Optimal Margin rate
11. Return $TTV\ threshold_i = \max(TTV_i)$
12. End

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5826
***Article Received**: 24 September 2022 **Revised**: 31 October 2022 **Accepted**: 10 November 2022*

Support Vector Machine (SVM)

In this section, the Support Vector Machine (SVM) is the classification technique by training the model with the authentication factors of legitimate device factors. The Support Vector Machine based classification is performed based on the hyperplanes so as to decide the class boundaries in input space or the border range with high-dimensional feature space. Further, the SVM mode involves constructing the linear functions based on the input or the feature space that is reflected on the hyper planes that are obtained from the features of training data. Specifically, the positive and negative data inputs are divided by the hyperplane. Moreover, the linear separator is framed from the hyperplane to the nearest value of positive or negative results with the larger distance. In particular, this produces instant results with appropriate classification of positive and negative samples, which may not be applied for the samples from test data.

In SVM, each input data is considered to be as in the row in the high- dimensional input or feature space, in which the attributes are considered to be the dimensionality of the feature-space. Moreover, the SVM training model provides the best separation of two classes using hyperplane with the obtained training samples. Non-linearity problems in support vector models are solved by using the high- dimensional space mapping for the n-dimensional input samples. From that, a linear classifier is derived which can perform the functions of a non-linear model with the n- dimensional input samples with the high-dimensional feature space. For performing that effectively, SVM is used in this model.

The simulation parameters and defined values are shown in table 2. The results are evaluated based on Packet Delivery Ratio (PDR), Transmission Delay, Residual Energy of nodes and Computational Overhead, with respect to two factors such as Monitoring Interval and Attack Frequency. The terminologies of the performance analysis are discussed.

RESULTS AND OBSERVATIONS

The model is implemented and evaluated using the Network Simulator called NS2 and the obtained results are compared with the Trust Management Model (TMM) [101]. It is assumed that the traffic flow is collected from 16 devices, comprising 12 IoT devices, 2 gateway points, 1 router, and 1 sink node as in figure 7.

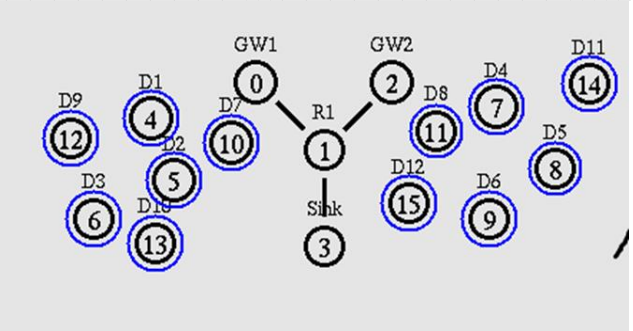

Figure 6 Simulation Topology

The simulation parameters and defined values are shown in

Packet Delivery Ratio (PDR)

PDR can be evaluated based on the rate of number of packets delivered to the total amount of data packets forwarded from source to target.

Transmission Delay

Transmission Delay is the delay that occurs when the packets are transmitted from source to destination.

Residual Energy

Residual Energy is the amount of energy that is remaining in each IoT devices after performing a certain task.

Computational Overhead

Computational overhead is the measure of complexity rate in the communication between the devices in the network

Table 2 Simulation parameters

Parameters	Values
Number of Nodes	16
Size of the topology	150 X 150
MAC Protocol	IEEE 802.15.4
Monitoring Interval	20,40,60,80, and 100sec
Traffic Source	Constant Bit Rate
Propagation	Two Ray Ground
Antenna	Omni Antenna
Initial Energy	10 Joules
Transmission Power	0.8 watts
Receiving Power	0.5 watts
Attack Frequency	50,75,100,125 and 150 kb/s

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 11
DOI: https://doi.org/10.17762/ijritcc.v10i11.5826
***Article Received**: 24 September 2022 **Revised**: 31 October 2022 **Accepted**: 10 November 2022*

EVALUATIONS BASED ON MONITORING TIME

The evaluations based on the monitoring time are very significant to measure the model efficiency. Moreover, in this work, the evaluation metrics are measured with increasing rate of monitoring time from 20 to 100 seconds and the results and comparison graphs are given below

Table 3 Results obtained for Delay against Monitoring Interval clearly depicts the delay value at every 20 seconds. Delay value is comparatively lower than the TMM Model. The delay is approximately 4 milliseconds in every time interval. Hence table 3 proved that TAAPML is better than TMM model with respect to delay. clearly depicts the delay value at every 20 seconds. Delay value is comparatively lower than the TMM Model. The delay is approximately 4 milliseconds in every time interval. Hence table 3 proved that TAAPML is better than TMM model with respect to delay.

Table 3 clearly depicts the delay value at every 20 seconds.

Evaluation Factors	Delay (ms)	
Monitoring Time (seconds)	TAAPML	TMM
20	38.84	42.32
40	39.07	411
60	39.16	433
80	39.19	44.32
100	39.21	44.33

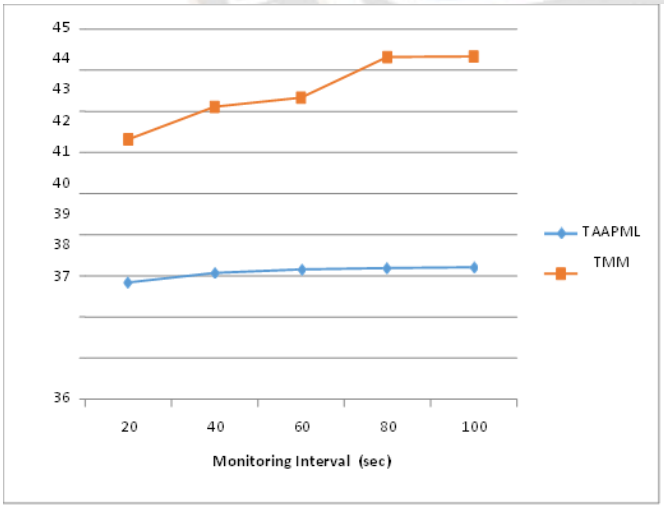

Figure 7 Delay Vs Monitoring Time

The figure 15 depicts that the overhead of TAAPML ranges from 92.03 to 275.99 and the overhead of TMM ranges from 142 to 452. Ultimately, the overhead of TAAPML is 41% less when compared to TMM. The results show that the proposed model achieves minimal overhead than the compared model.

Conclusion

From the graphs, it is depicted that the proposed model achieves 10% lesser delay, 1.3% better rate of delivery ratio, 1.28% of more residual energy and approximately lesser overhead of 11% than the compared TMM model. It shows that the proposed model outperforms the compared one when it is analyzed with Monitoring Interval factor , which is evaluated at the rate of, 20, 40, 60, 80, and 100 seconds.

From the graphs, it is depicted that the proposed model achieves 16% of lesser delay, 1% better rate of delivery ratio, 1.8% of more residual energy and approximately 41% of lesser overhead than the compared TMM model. It shows that the proposed model outperforms the compared one when it is analyzed with the attack frequency factor, which is evaluated in the rates of 50, 75, 100, 125 and 150 in kb/s.

The graphs show that the proposed model outperforms the compared existing model in all directions of evaluations. Further, the second phase of this work is to define a novel model for tightening the security process of data communication in IoT by incorporating advanced cryptographic operations and key generation functions.

References

[1]. Naresh P and Debasis D, 2017, “Algorithm for Trust Based Policy Hidden Communication in the Internet of Things,” IEEE Computer Society, Vol-4, pp. 148-153.

[2]. ZeeshanA K , Johanna U , Artemios G. Voyiatzis, and Peter H , 2017, “A Trust-based Resilient Routing Mechanism for the Internet of Things,” ACM International Conference on Availability, Reliability and Security, Vol.27 pp. 1- 6.

[3]. Upul J , GyuMyoung L , Tai-Won Um, Qi Shi, 2019, “Machine Learning based Trust Computational Model for IoT Services,” IEEE Transactions on Sustainable Computing, Vol-4, pp. 39-51.

[4]. António P and Ricardo C 2016, “Hash-Chain-Based Authentication for IoT,” Advances in Distributed Computing and Artificial Intelligence Journal, Vol.-5, No. 4, pp. 43-57.

[5]. Khirod C S and Umesh C P, 2017, “IoT Based Intrusion Detection System Using PIR Sensor,” 2nd IEEE International Conference On Recent Trends in Electronics Information-&-Communication-Technology), pp. 1641-1645.

[6]. Rohan D, NoahA and Nick F, 2018, “Machine Learning DDoS Detection for Consumer Internet of Things Devices,” ArXiv Journal Publications, pp. 29-35.

[7]. Hanif R, Jinshan L and Jung-M (Jerry) Park, 2018, “Secure Match: Scalable Authentication and Key Relegation for IoT Using Physical-Layer Techniques,” IEEE Conference on Communications and Network Security, pp. 1-9. 146

[8]. Zheng, Dehua; Hong, Zhen; Wang, Ning; Chen, Ping. 2020, “An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application,” Sensors Vol.20, No. 6.

[9]. Otoum, Yazan& Liu, Dandan&Nayak, Amiya. 2019, "DL-IDS: A Deep Learning–Based Intrusion Detection Framework For Securing IoT," Transactions on Emerging Telecommunications Technologies, Vol.30 No.11.

[10]. Yulong Fu, Zheng Yan, Jin Cao, OusmaneKoné, Xuefei Cao 2017, "An Automata Based Intrusion Detection Method for Internet of Things," Mobile Information Systems, Vol,2017, pp.1-13.

[11]. Hamza, Ayyoob&HabibiGharakheili, Hassan &Sivaraman, Vijay. 2018, "Combining MUD Policies with SDN for IoT Intrusion Detection," Proceedings on IoT Security& Privacy". pp 1-7.

[12]. M. Azarmehr, A. Ahmadi and R. Rashidzadeh, 2017, "Secure Authentication and Access Mechanism for IoT Wireless Sensors," IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, 2017, pp. 1-4.

[13]. C. Guo, R. Zhuang, Y. Jie, Y. Ren, Ting Wu and K.K. R.Choo, 2016, "Fine- Grained Database Field Search using Attribute-Based Encryption for E-healthcare Clouds," Journal of Medical Systems, Vol. 40, No. 11, pp. 1-8.

[14]. Y. Yang, 2015, "Attribute-Based Data Retrieval with Semantic Keyword Search for e-Health Cloud," Journal of Cloud Computing, Vol. 4, No. 1, pp. 1-6.

[15]. N. Shekokar, K. Sampat, C. Chandawalla and J. Shah, 2015, "Implementation of Fuzzy Keyword Search over Encrypted Data in Cloud Computing," Procedia Computer Science, Vol. 45, pp. 499-505.

[16]. Z. Fu, J. Shu, X. Su and D. Zhang, 2014, "Semantic Keyword Search Based on Tier over Encrypted Cloud Data," Proceedings of the 2ndInternational Workshop on Security in Cloud Computing, ACM, pp. 59-62.

*Corresponding Author