International Journal For Technological Research In Engineering
Volume 10, Issue 8, April-2023 *ISSN (Online): 2347 - 4718*

ANALYSIS ON TRUST MANAGEMENT SERVERLESS TECHNIQUES FOR GREEN CLOUD COMPUTING & INTERNET OF THINGS

Aishwarya Shekhar
Research Scholar
SCSE, Galgotias University
Greater Noida, India

Abstract*—Internet of thing is a new technique through which the devices are connected through each other with the help of internet. The nodes that can process and retrieve data from other devices with or without human interference are called sensors or actuators. The development of IOT brings a significant change in the various areas like The smart cities, The smart healthcare, The smart transportation, in cellular communications, in data mining, in manufacturing, and lastly in environmental monitoring. By using various methods Trust management in an IOT environment is provided which employs past experience, sensor data irregularity, reliability, and availability as trust matrices. IOT faces new problems day by day due to its particular features. The most important of these features, apart from privacy and security, is trust and to manage server less trust management. Various Techniques have been developed to know about how the IOT generated data is being converted into useful information to provide a secured and trustworthy communication.

***Keywords*—Green Cloud Computing, Cloud Computing, Trust Based Techniques, Serverless, Internet of Things**

I. INTRODUCTION

IOT is an emerging technology that provides a base to replace the traditional communication systems with a modern one. In this system, machines perform different operations to handle changing situations in real life without the involvement of human efforts. IOT permits nodes to have different characteristics and share services and information. Things produce decentralized networks with adaptable topologies. In this specific situation, it is essential to have a strong, versatile and reliable communication, and correspondence among these devices. Various devices like computers and mobile phones work together to make humans life more comfortable. With this rising number of connected devices, it is hard to assume that which device is Trustworthy. These 26 are the trust management techniques used for Secured and Trustworthy communications of the data generated by IOT devices. a.E.Lithe b.GTRS c.TWGA d.TBBS e.MAG-SIoT f.ATES g.TMSMD h.DTMS i.SMA j.ABAC k.ATBP l.DCTEPF m.TrustCEP n.MAPE-K o.TDFDS p.CBSTM-IoT q.Timely-Trust r.DTRM s.ANTs t.TAS-IoT u.CTM-IoT v.TMCol-SIOT w.DTEB x.CTMS-IoT y.TMF-VSN z.IOT-HITrust.

IoT manages the concept of connecting billions of tiny electronic devices to retrieve and share information regarding numerous applications, such as healthcare, environment, and industries among others. In contrast, IOT has unproven characteristics (for example, security, privacy, and trust), which are crucial in some environments such as VANETs (Vehicular ad hoc network) [1].

II. BACKGROUND

IoT is an emerging technology that provides a base to replace the traditional communication systems with a modern one. In this system, machines perform different operations to handle changing situations in real life without the involvement of human efforts. IoT permits nodes (things) to have different characteristics and share services and information. Things produce decentralized networks with adaptable topologies. In this specific situation, it is essential to have a strong, versatile and reliable communication, and correspondence among these devices. Various devices, for example, computers and mobile phones, work together to make humans life more comfortable. With this rising number of connected devices, it is hard to assume that which device is trustworthy. For this reason, several approaches have been developed[2-14].

A. E.Lithe

Enhances security for constrained devices that in turn decreases Dos attacks by sharing secret keys. In this technique, a secret key is shared between two devices to avoid DoS attacks and therefore the security for constrained devices is increased. However, if an intruder creates multiple requests from different devices, the battery drainage becomes crucial to handle frequent computations .

B. GTRS

The GTRS follows the idea of social IoT where a node sends a request towards its friends to get recommendations for the past ratings. If the best rated node is found then it is selected, otherwise, the request is forwarded to the friends-of-friends. Thus, all nodes are capable to calculate their own predictions for the best rated services. Nevertheless, the system is unable to predict the rating of a device if it has not been rated. GTRS computes the effectiveness of one node on another by combining their trust and similarity.

C. TWGA

The TWGA consists of four components, i.e. i) path establishment among trust domains, ii) data forwarding to

smart homes, iii) usage of public or private keys to identify the correct ID-packet, and iv) route selection through the ID-packet engine. Hence, the scheme provides useful security through public/private keys, but cannot avoid the repudiation attacks if an intruder injects false data.

D. TBBS

The TBBS includes IoT enabled vehicles, traffic signals, and speed detectors to control data transfer among vehicles. Every vehicle has a default trust value that can be used in the future if needed. The TBBS may be helpful in selecting a particular route, however, this is a proposed approach and therefore it is early to predict its performance and accuracy without deployment

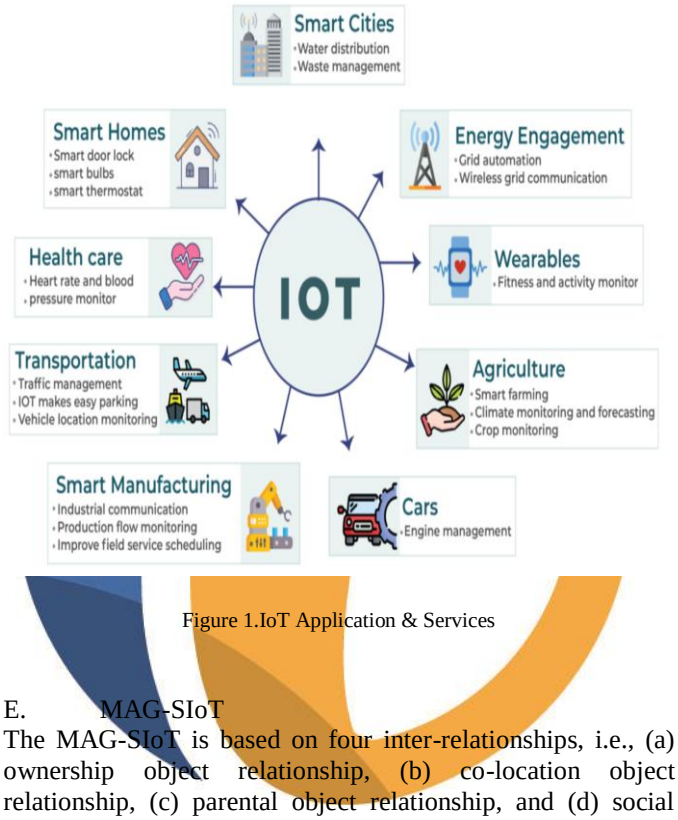

Figure 1.IoT Application & Services

E. MAG-SIoT

The MAG-SIoT is based on four inter-relationships, i.e., (a) ownership object relationship, (b) co-location object relationship, (c) parental object relationship, and (d) social object relationship. The trust in this model is calculated on the basis of trust metrics, which include social relationships and the context in which the relationship is communicated. Therefore, this model is suitable to establish the relationship based on nodes' affinity, but it is inappropriate when the number of attributes increases.

F. ATES

The ATES is designed to calculate both personal and non-personal trust values of IoT devices. The personal trust value of a device is calculated in three ways, i.e., i) the current situation of a device, ii) from the experience history of a device, and iii) through M5 tree regression model. Whereas the non-personal trust value is computed with the help of other users' experience. Thus, the model can produce the ideal trust value in case of first time interaction with other devices. However, the accuracy of results depends on more number of situational characteristics.

G. TMSMD

In the TMSMD model, the trust is maintained at each layer of the network. The Physical layer provides data integrity and privacy, while the Application layer keeps the confidentiality of services. This model develops trust by reducing overhead and uses a public key to protect data. However, it consumes maximum power because it uses the public key cryptography, which is based on the integer factorization.

H. DTMS

The DTMS is based on a distributed mechanism to provide various services in the IoT environment. The trust value of each node is calculated on direct observations. The service provided by each node has a reward if it is provided on time, and a penalty if it is not provided to the nodes. This model performs well to evaluate selective attacks in a trust management model, but it increases the chances of Bad-Mouthing attacks.

I. SMA

The SMA is designed to provide an automatic method to identity IoT devices, calculate their semantic attributes, and estimate their trustworthiness. The architecture includes two parts, i.e. the smart middleware architecture and the semantic device discovery with trust evaluation. The middleware architecture calculates the trustworthiness and semantic discovery of IoT objects based on their text attributes. The SMA is more trustworthy as it extracts text and numerical data from IoT devices through the network. However, it increases computational over head as it uses textual and numerical information for the discovery of resources and calculation of trust score.

J. DTEB

The DTEB system was designed to time stamp digital documents. The system works on Smart Contract that uses the Blockchain architecture, which consists of four layers, i.e., Interactive layer, Management layer, Network layer, and Data layer, for exchanging data in a trusted environment. The DTEB system is transparent and immutable to record a transaction, but there are still privacy issues that make the IoT environment untrustworthy.

K. ABAC

The ABAC model was proposed to keep data protected from malicious nodes. The system comprises three modules, i.e., trust evaluation, access decision, and authentication. Thus, it provides a secure authorization because the trust level changes with the behavior of nodes. However, the system accuracy cannot be predicted if one device interacts simultaneously with several other devices.

L. ATBP

The ATBP is developed to allow security measures among nodes of a social network. The model adopts a trust policy that is followed by all network nodes. The ATBP suggests an application for travelers, known as map guide, who can be installed on a Smartphone for the calculation of trust either directly or indirectly. It considers the honesty as a trust property for managing Bad-Mouthing attacks. The model is useful in deciding the best route so as to avoid traffic

congestion and accidents, and provide safe and smooth drive. Though the travel map guide application gives an easy access to applications, but it may be hindered in high dynamic situations.

M. DCTEPF

The DCTEPF system consists of various modules, for example, trust data access object, trust service enabler, decision making and prediction, trust agent, data repository, Trust Computation, and API, to calculate the trust. This system is useful to filter out inaccurate data. Nonetheless, it is not helpful to handle contextual information for trust predictions.

N. TrustCEP

The TrustCEP is divided into two parts: The producer and the consumer, which are connected through the operator graph. This model is based on mutual trust between two users. Every user tries to find neighboring users and looks into their trust vectors. If there are no neighboring users then the graph is initiated on their own device and requests are placed for collaborating placement requests. However, it fails to provide support in a scenario with a higher mobility.

O. MAPE-K

The MAPE-K approach was proposed to handle the dynamic environment. In the IoT Cloud environment, this scheme is cooperative as it provides facility to tackle malicious recommendations from other nodes. For quick response, the idea of distributed trust agents is used in the MAPE-K feedback loop. The proposed model helps increasing the dynamic trust management level through a self-adaptation method. Yet, the problem occurs if data attributes increase from the threshold.

P. TDFDS

The TDFDS model consists of four modules that define various variables of trust, i.e., customer, business requirement, and technology. The environment variable involves technological attributes as well as social, cultural, and religious factors. The customer variable includes human intelligence and their physical abilities. The business requirement variable includes attributes that affect the trust. And the technology attribute maintains system's security and usability. The primary purpose of TDFDS is to provide trust for online integrated and distributed applications, but during application running, it does not provide security for administrators

Q. CBSTM-IoT

The CBSTM-IoT is designed for the nodes' collaboration and to limit interactions of suspicious devices. In this model, if the relationship value is high, it indicates a higher trust. As the CBSTM-IoT model does not depend on specific nodes and peers, malicious nodes may allocate higher trust values to other nodes as indirect recommendations.

R. Timely Trust

The Timely Trust framework identifies the demand of IoT in GVTs and tells that how the swift trust formation in GVTs is affected by different cultures. GVTs have common shared objectives on which they work across geographical boundaries and depend on technology such as computers to communicate. They do not have any previous working record with each other and also have cultural differences. Due to embedded IoT concepts, the GVT members can easily communicate through video calls or voice messages. However, the sharing of data on remote servers over different regions increases the chances of cyber-attacks.

S. DTRM

The DTRM focuses on distributed environment to make IoT devices capable of handling processing. The model also proposes different levels of security, which are suitable for sensitive devices in the IoT environment. It keeps record of all devices and manages them according to their requirements. It provides protection against Bad-Mouthing, Good-Mouthing, and ballot attacks, but fails to handle some attacks, such as DDOS, MIM, and wormwhole.

T. ANTs

The ANTs divides the network into trust zones for checking new joining nodes and reconfigures the existing trust zones. The reconfiguration of trust zones helps restricting remote communications and safeguarding the network from several kinds of attacks. In the ANTs, the ED becomes part of the network and allows all nodes to communicate over a secure channel using SHGW. The SHGW works as a monitoring device to identify and exclude malicious nodes from the network. However, scheming suitable policies and procedures to put EDs into the trusted zones is a challenging issue.

U. TAS-IoT

In the TAS-IoT model, nodes are divided into two categories, i.e., legitimate nodes and non-legitimate nodes. The legitimate node appends on authenticator for authenticating messages. It prevents non-legitimate nodes to post false messages in the network and therefore reduces power consumption by authenticating data at its origin. A trust value is associated with each node on the basis of observations, experience, and recommendations. After the trust value is calculated, an adaptive function is used to decide if a message needs authentication.

V. CTM-IoT

The CTM-IoT is designed for reliable information sharing among IoT nodes. The IoT network is divided into different clusters, where each cluster includes a trust manager, i.e., a master node. The model also comprises a super node which stores trusted data of all master and cluster nodes in the central repository. In addition, the super node also monitors traffic and trust management among all IoT devices. Moreover, it shares data packets between the master node and cluster nodes, and the IoT applications and the master node. This model can achieve the primary goal of trust management among IoT devices however, without comparison with other schemes it is difficult to predict its supremacy over the existing available techniques.

W. TMCoI-SIoT

The TMCoI-SIOT is designed to integrate various characteristics of trust on the basis of direct and indirect

evaluations. The proposed architecture employs the idea of clustering and divides nodes into communities on the basis of interest, where the network consists of an SIoT server, nodes that are clustered together as a community, and a trust administrator for security management. If a node needs to join the network, the SIoT server authenticates it. After the authentication, the node may join the community of its own interest or either it can start creating its own community. The TMCoI-SIOT helps to reduce challenges associated with memory storage however, it cannot eliminate Bad-Mouthing and Good-Mouthing attacks.

X. CTMS-SIoT

The CTMS-SIOT is designed to consider dynamic trust values together with a relative context in different tasks. This model is based on computational complexity, where a node's life time decreases because of information caching in a decentralized architecture. The CTMS-SIOT includes two modules, which are responsible for contextual trust and reputation. A trust request from a user activates the discovery mechanism, where lack of history in the local trust table compels a user to send a trust request query to the server. As the server receives a request, the entity selection process is initiated based on the past experience. The CTMS SIOT is used to compute social similarities between the requester and the selected node. The model provides a dynamic environment through effective services, but it reduces the system trustworthiness.

Y. TMF-VSN

The TMF-VSN is proposed for VSN, which includes three layers of trust for the VSN environment, i.e., GTM, DTM, and VTM. The GTM lies on the top level and holds the authentication of vehicles' profiles. The DTM holds the history, domain, and relationship profiles of each individual vehicle. While the VTM is used to maintain vehicles' information. The proposed model includes four modules, i.e., friend trust, neighbor trust, global trust, and history trust modules for the trust evaluation. The system can improve the performance of network by increasing the packet delivery ratio, but the validity of experiments may be affected due to nodes' density.

Z. IoT- HiTrust

In the IoT-HiTrust, the trustworthiness of all IoT devices is calculated by a cloud in the region of cloudlets. The system is divided into three layers, i.e., the cloud layer, the cloudlet layer, and the device layer. At the cloud service level, each IoT device has a unique identity, which is used to manage users' data. The home cloud server of a user remains the same, however, its VM may be shifted from one point to the other. In case, each owner has multiple devices, then all devices are mapped to the owner home cloud. Devices' requests and replies are communicated only inside their cloudlet regions together with their stored information. If the Internet connection is terminated then a cloudlet replies user queries inside the region with a disconnection mode. Furthermore, if a user moves from one cloudlet to the other then it is removed from the previous cloudlet and is registered in the new one. The proposed model achieves an appropriate trust in a large IoT system, but it does not succeed to control intruders as it ignores the intrusion detection.

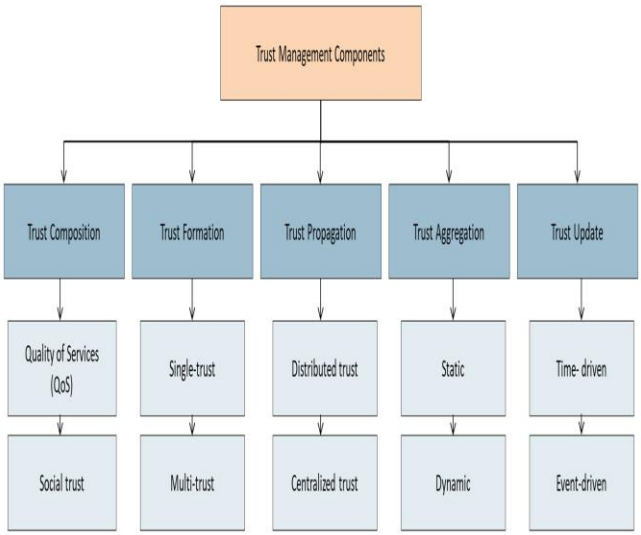

Figure 2. Trust Management Components

III. CONCLUSION

In the IoT system, devices perform various tasks to handle real life situations without human intervention. Therefore, without human interactions, it is indispensable to have a strong and reliable communication among these devices. In other words, the deployment of trust among IoT devices is utmost important for a smooth and fair data transmission. IoT allows the concept of connecting billions of tiny devices to retrieve and share information regarding numerous applications, such as healthcare, environment, and industries among others. In contrast, IoT has unproven characteristics (for example, security, privacy, and trust), which are crucial in some environments such as VANETs. This paper surveys trust management techniques designed for the Internet of Things (IoT). On the basis of comprehensive analysis of trust management, relevant techniques are classified and their contributions and limitations are presented. We expect that this survey will be effective for the IoT research community, working on trust management, to comprehend the viewpoints and issues that IoT faces in trust administration.

REFERENCES

[1] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, ''Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey,'' IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2546–2590, 4th Quart., 2016.

[2] R. Minerva, A. Biru, and D. Rotondi, ''Towards a definition of the Internet of Things (IoT),'' Tech. Rep., 2015. [Online].

[3] A. Gharaibeh et al., ''Smart cities: A survey on data management, secu rity, and enabling technologies,'' IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2456–2501, 4th Quart., 2017.

[4] G. Acampora, D. J. Cook, P. Rashidi, and A. V. Vasilakos, ''A survey on ambient intelligence in

healthcare,'' Proc. IEEE, vol. 101, no. 12, pp. 2470–2494, Dec. 2013.

[5] S. Pellicer, G. Santa, A. L. Bleda, R. Maestre, A. J. Jara, and A. G. Skarmeta, ''A global perspective of smart cities: A survey,'' in Proc. 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), 2013, pp. 439–444.

[6] M. Elsaadany, A. Ali, and W. Hamouda, ''Cellular LTE-A technolo gies for the future Internet-of-Things: Physical layer features and chal lenges,'' IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2544–2572, 4th Quart., 2017.

[7] C.-W. Tsai et al., ''Data mining for Internet of Things: A survey,'' IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 77–97, 1st Quart., 2014.

[8] Aishwarya Shekhar, A Very Robust Dedicated and Verified Technique by Applying the Hybridity of Cloud for Deduplication of Data: IJTRE,2016

[9] N. Zhao, F. R. Yu, H. Sun, A. Nallanathan, and H. Yin, ''A novel interference alignment scheme based on sequential antenna switching in wireless networks,'' IEEE Trans. Wireless Commun., vol. 12, no. 10, pp. 5008–5021, Oct. 2013.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ''Internet of Things (IoT): A vision, architectural elements, and future directions,'' Future Generat. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[11] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, ''Context aware computing for the Internet of Things: A survey,'' IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.

[12] M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, ''The virtual object as a major element of the Internet of Things: A survey,'' IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1228–1240, 2nd Quart., 2015.

[13] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, ''A survey on network methodologies for real-time analytics of massive IoT data and open research issues,'' IEEE Commun. Surveys Tuts., vol. 19, no. 3, pp. 1457–1477, 3rd Quart., 2017.

[14] Z. Yan, P. Zhang, and A. V. Vasilakos, ''A survey on trust management for Internet of Things,'' J. Netw. Comput. Appl., vol. 42, pp. 120–134, Jun. 2014.

