International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

Policy-aware Distributed and Dynamic Trust based Access Control Scheme for Internet of Things

Poonam Ninad Railkar[a,*], Parikshit Narendra Mahalle[b], Gitanjali Rahul Shinde[c], Nilesh P. Sable[d]
[a,*]Computer Engineering, Smt. Kashibai Navale College of Engineering, SPPU, Pune, India
E-mail: poonamrailkar@gmail.com
[b]AI & DS, Vishwakarma Institute of Information Technology, SPPU, Pune, India
E-mail: aalborg.pnm@gmail.com
[c]Computer Engineering, Vishwakarma Institute of Information Technology, SPPU, Pune, India
E-mail: gr83gita@gmail.com
[d]Information Technology, Vishwakarma Institute of Information Technology, SPPU, Pune, India
E-mail: drsablenilesh@gmail.com
*Corresponding author *E-mail: poonamrailkar@gmail.com

Abstract
The use of smart devices is driving the Internet of Things (IoT) trend today. Day by day IoT helps to support more services like car services, healthcare services, home automation, and security services, weather prediction services, etc, to ease user's life. Integration of heterogeneous IoT devices and social resources sometimes creates many problems like the privacy of data. To avoid privacy issues, an appropriate access control mechanism is required to check authorized and trusted devices, so that only valid devices can access the data which is only required. In the sequel, this paper presents implementation of distributed and dynamic trust based access control mechanism (DDTAC) for secure machine to machine communication or distributed IoT environment. Novelty of this mechanism is that, it uses trust calculation and device classification for dynamic access control. The proposed scheme is implemented, tested and deployed on Node MCU and same mechanism is also simulated on NS-2 for large number of nodes. This access control model support Scalability, Heterogeneity, Privacy, Trust, Selective disclosure, Principle of least privileges, and lightweight calculation features. Results of this models proves that it gives good performance as compared to existing scheme in terms of scalability, throughput and delay. As number of devices increase it does not degrade performance. This mechanism is also protected against the Man-in-the-Middle attack, Sniffing attack, Session Hijacking attacks and Injection attacks. It required less time to detect and resist those attacks.

Keywords: Access control, Decentralised Identifier, Internet of Things, Machine to Machine communication, Selective disclosure, Trust Management.

1. INTRODUCTION

The term phrase "Internet of Things" (IoT) is firstly introduced by Kevin Ashton in 1999 [1]. IoT is a collection of devices that is embedded with sensors, actuators, communication technologies, and software to process and exchange data to other devices over a network. A global infrastructure for the information society that connects physical and virtual devices, smartphones, RFID tags, using existing and emerging interoperable information and communication technologies to provide advanced services [2].

With the tremendous change in IoT technologies, billions of devices are communicating with each other to provide services [3]. Emerging in IoT technologies, multiple service domain communicates with each other over the internet and provides useful services. Figure 1 shows converged IoT use case where multiple users accessing multiple services over access network, so this access network can be Bluetooth, Wi-Fi, 3G, 4G etc. Over this access network, there is need to protect resources, credentials, and services. In Machine-to-Machine communication (M2M) every device is connected to the sensors that cause the control system to send instructions to a specific machine to perform an action automatically with less or without human intervention [4]. This network will link to the internet through both wireless and wired connections.

Access control system ensure who (usually user/ devices) can access what (usually operation) on which devices. In short which subject access what operation on which objects. In IoT network many nodes are moving from one network to another so there is need of dynamic access control. For these new devices, prediction of access control in advance is very difficult. So, effective dynamic access control is needed for such scenario [5]. As Dynamic Access Control is used, if a device trust and capacity changes, the device permissions shift dynamically without the need for additional administrator intervention [6].

The remaining paper is organized as follows. Firstly, Section 2 provide related work, and critical gap analysis. Then accesso control policies in Section 3. Proposed Access Control model

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

discussed in section 4. Implementation details is given in section 5. Section 6 discusses the result and discussion. Section 7 concludes the paper and provides the future scope of the project.

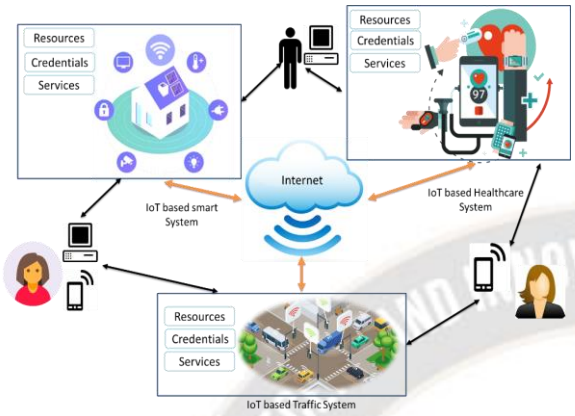

Figure 1: Converged IoT use case

2. RELATED WORK

DACIoT [7] system gives dynamic access control. This system extends the eXtensible Access Control Markup Language (XACML) and supports Automatic policy generation, Continuous policy enforcement, and adaptive policy adjustment functionalities. The results of system shows that it scales well in IoT environment and security is improved.

System [3] is responsible for monitoring the devices and gathering trust metrics such as successful forward ratio (SFR), data integrity (DI), and energy consumption rate (ECR). These trust parameters are then merged with the help of a fuzzy engine, and an overall trust value is determined. The mechanism of access control is determined on the basis of the trust value. They have demonstrated the results of the simulation using NS-2, and that this TAACS-FL is expandable and uses very little energy.

Author in [8] proposes attribute-based access control using blockchain. In their scheme attributes are distributed over blockchain. Their scheme is trustworthy as no one can tamper the data. Their system also effectively resists against impersonation attack, collusion attack, and MITM attack and they have checked security analysis on AVISPA tool.

[9] extended role-based access control mechanism by adding security related context information like time, state of environment, location which helped in access decision. Authors in [10] used role-based access control mechanism along with social network profiles for creating access control policies in Web of Things. Paper [11] proposed mutual authentication and fine-grained attribute-based access control mechanism for resource constrained environment. [12] also proposed UCON based access control scheme for distributed and dynamic IoT environment. UCON scheme involves authorizations, obligations, conditions, continuity, and mutability. It is conceptual model based on fuzzy theory.

Author in [13] used Elliptic Curve Cryptography optimizations for capability-based access control for constrained and smart devices. Their solution is lightweight and support scalability, interoperability, and security. This scheme is validated on AVISPA tool and implemented in a real testbed based on the Jennic/NXP JN5148 module

The article [14] outlines a fuzzy approach to Trust Based Access Control for the purpose of identity management. This technique is founded on the idea of trust degrees. The findings of the simulation indicate that the fuzzy methodology to trust-based access control is both scalable and efficient in terms of energy consumption. In conjunction to this, the study proposes the use of trust in order to provide dynamic identity management in decentralized IoT. It is both convenient and scalable to use because the platform's functionality and effectiveness are unaffected by the amount of devices that are connected to it.

A comparative examination of several access modulation schemes enabling machine-to-machine communication in the internet of things is presented in [4]. During the gap analysis, they identified important characteristics such as confidentiality, scalability, confidence, and heterogeneity and then performed a comparative study of various access control approaches on the basis of these factors. They have also suggested a scalable system for access control based on trust score. The proposed mathematical model takes into account a variety of factors in the development of a trust management system.

The authors in [15] present protocol of trust model for access control in dynamic or pervasive devices. The initial implementation of this protocol was developed using XACML. Idea behind this protocol is to add atomization and reduce need of centralized admirations.

We conducted a gap analysis, the results of which are presented in table 1, and determined the essential components and prerequisites for an effective access control system. The following are the conditions that must be met:

1. Capacity to Scale: Since a big number of Internet of Things apps are installed on a large number of different devices, the access control mechanism must be able to accommodate this growth.
2. Heterogeneity: Numerous applications call for the utilisation of a wide variety of sensors and other sorts of devices. These devices each employ a distinct heterogeneous technology, have a unique capacity for computing, and have varying requirements for their energy sources.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
Article Received: 24 August 2022 Revised: 29 October 2022 Accepted: 22 November 2022

TABLE 1: COMPARATIVE SUMMARY OF THE STATE OF ART FOR ACCESS CONTROL

Access Control Model	Scalability	Heterogeneity	Privacy	Trust	Selective Disclosure	Principle of least privileges	lightweight calculation	Distributed	other feature
DACIoT [7]	High	High	No	No	No	NO	medium	Yes	Automatic policy generation, Continuous policy enforcement, and adaptive policy adjustment functionalities
TAACS [3]	High	High	Medium	Yes	No	No	Yes	Yes	energy efficient
ABAC using blockchain [8]	High	High	Low	Yes	No	No	Yes	Yes	flexible, dynamic and fine-grained access control
RBAC [9],[10]	Medium	High	Low	No	No	No	No	No	proposed extended role-based access control by incorporating the context information
	Medium	High	Low	Yes	No	No	Yes	No	integrate SNS into Role-Based Access Control Model in web of Things
ABAC [11]	Medium	Medium	Medium	Yes	No	No	Yes	Yes	-achieve flexible fine-grained access control. -Defend against man-in-the-middle attack, eavesdropping attack, node capture attack
UCON [12]	Low	Medium	High	Yes	No	No	No	Yes	It is conceptual model based on fuzzy theory
CAPBAC [17],[13]	High	Low	Medium	Yes	No	No	Yes	Yes	secure authority delegation for highly distributed system.
	High	Low	Medium	No	No	Yes	Yes	Yes	Elliptic Curve Cryptography optimizations Flexible, interoperability and end-to-end security
LCap [18]	High	High	No	No	No	No	Yes	No	efficient format for capability tokens that is used fully stateless and decentralized
Proposed Model	**High**	**High**	**High**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	Attack Resistant, Dynamic access control

3. Privacy: Methods of access control should be designed with privacy in mind in order to ensure that users do not put their own information at risk.

4. Trust: Trust is an essential component of M2M communication in the IoT, as it enables secure connection between two devices. because the dynamic environment of the internet of things requires a runtime way to define trust.

5. Selective Disclosure: Before consumers may make use of many services (or goods), providers must first gather a certain quantity of personal data, which is typically rather substantial. Many users, on the other hand, prefer to have complete control

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

over the information they make public. This trend strongly suggests that services provide support for selective disclosure.

6. The principle of least privileges: The principle of least privileges, also known as the principle of negligible privilege or the principle of least authority, requires that in a general and especially abstraction layer of a computing environment, every module (such as with a process, a user, or a programme, depending on the subject) would have to be able to access only the information and resources that are needed for its legitimate purpose [16]. The principle of least privilege is also known as the principle of minimal privilege or the principle of least authority.

7. lightweight calculation: Very simple formulae are used find out trust between devices.

8. Distributed: In distributed networking resources are shared in different network.

3. ACCESS CONTROL POLICIES MODELLING

In the scope of this paper, office automation use case is considered for discussion. Here simple office automation IoT scenario is implemented.

Following Access rights are considered.

Access Right(AR) ∈ {Read, Read-Write, Execute, Print, NULL}

Different AR set represent by {∅, {Read}, {Write}, {Execute}, {Read, Write}, ….{Read, Write , Execute}}

Device type (DT) and trust score are classified as follows,

Device Type(DT) ∈{ Expedient device, Semi-Expedient device, Non-Expedient device}

Trust score category ∈{High, Medium, Low}

In reality, Expedient device have capacity of {Full access} but depend on trust score, access permission is changed. Similarly, Semi-Expedient device have {Read, write} and Non-Expedient device have {Read} capability but depends upon device type and trust score access permissions are mapping for device m to device n in equation (1):

Permission level of device $_{m \to n}$ α ***(weighted Trust score of device*** $_{m \to n}$ ***&& Device type) ……..(1)***

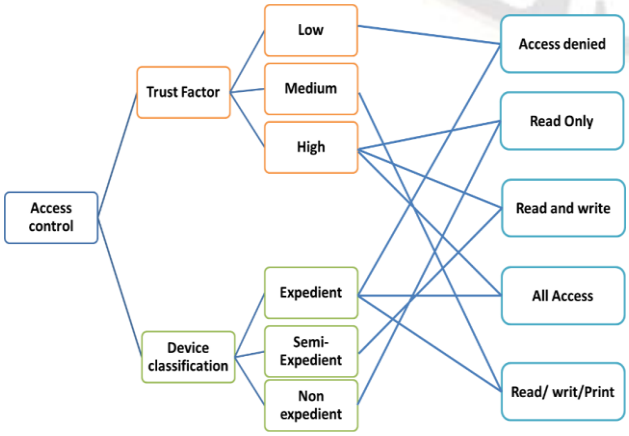

Figure 2: Permission mapping mechanism

Traditionally administrator creates permissions manually one by one for each device which is time consuming task. In DDTAC system permissions are generated based on trust calculation and device classifications as shown in figure 2.

Here we will give you overview of access permission. In our system trust factor of device can be Low, Medium or high and devices classified as Expedient, Semi-Expedient or Non-Expedient device. Now if devices are expedient device (means having full capability) but trust score is low then that device will get only Read permission. For example, in this case Laptop, which is capable but due to its previous interactions its trust score is low. And Vice versa if Non expedient device (means not powerful device and capability is less) having high trust it will also get read only permission. For e.g Printer is non expedient which does not require write and execute permissions. So, this situation also supports features of principle of least privileges. Even for expedient and high trust device if request is to read only for particular object (for E.g., Particular file) then ready only permission will be given. Here also principle of least privileges is applied. After successful of each interaction trust score is updated.

4. PROPOSED ACCESS CONTROL MODEL

Before applying access control authentication takes place. In the system that is being suggested, each gadget will have a decentralised identifier (DID). DID is like Self- Sovereign Identity (SSI). DIDs are completely autonomous from any centralised registry, identity provider, or certificate authority and are solely in the control of the individual who has been assigned the DID. DIDs are URLs that tie a DID subject to mechanisms for trustable interactions with that subject [19]. [Note: URLs are not the same thing as DIDs.] A DID is a straightforward text string that is divided into the following three sections: 1) the identification for the URL scheme, which is denoted by did; 2) the identifier for the DID Method; and 3) the identifier that is unique to the DID Method. Authentication is carried out based on the DID, which then enables selective disclosure. Validation of each individual device's decentralised identification is required for authentication purposes. If it is not authenticated then access control system will not initiated and if authenticated then DDTAM system will check its access permission based on device type and trust calculations as shown in figure 3.

Architecture of DDTAM supports feature like Scalable, Selective Disclosure, Principle of least privileges, Attack resistant, Trust calculation and device classification. Trust calculation for devices is done using fuzzy approach in DDTAM system. Parameters Experience (E), Recommendation (R) and Device classification (D) are used to calculate trust score of devices. Detail explanation of trust score calculation is out of scope of this paper, so for detailing refer paper [6].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

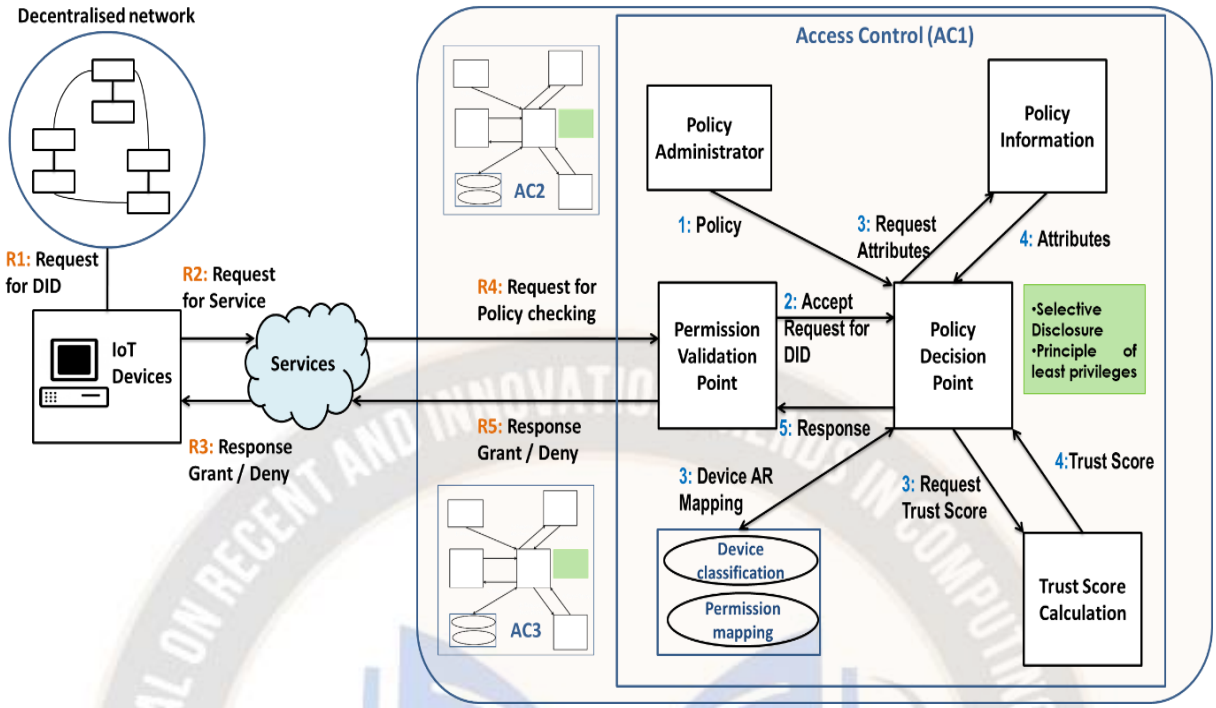

Figure 3: Proposed Architecture of Distributed and Dynamic Trust based Access Control (DDTAM)

A demand to acquire the capabilities of another device or service is sent from a smart device. Every gadget may be placed into one of three categories: expedient, semi-expedient, or non-expedient. Because when device receives a request for access, it first determines the trust score of both the device being requested access and then determines the kind of device being requested access from. Permission mappings will take place dynamically, and they will be determined according on data from applications and trust score calculation. This strategy will provide support to the concept of least privileges, which states that only the resources absolutely necessary to fulfil a request will be allotted for that purpose.

5. IMPLEMENTATION DETAILS

Algorithm 1 gives idea of how access permission is granted or denied

Algorithm 1: Automatic Access Policy Specification

```
1   Procedure ACCESSRIGHTS(DID, RS)
2   TS <-getTrustScore(DID)
3   DT <-get DeviceType(DID)
4   Service <-getReuestType(RS)
5   Policy <- checkPolicies(TS, DT, Service)
6   Decision <- listofPolicies(Policy)
7   If Decision != Access_Denied then
8   send(Allow Read ||read write||execute response)
9   else
10  Send(Deny Response)
11  end if
12  End Procedure
```

In algorithm 1 for ACCESSRIGHTS function input will DID of device and its service request. For that device trust score is taken from trust score component and device type from device classification component. Then it checks which type of service request is there. So based on Trust, device type and service, policy will be given. This service type is required here to provide principle of least privileges. Depend on policies, decision is given. If decision is not equal to access denied then permit for operation otherwise denied permission.

Main Controller of DDTAC system is NodeMCU. Trust based Access control is executed on NodeMCU. At the time of execution network consist of Laptop, smart phone, Multifunction printer, Bluetooth, and router. Screenshot in figure 4 shows list of polices considered in DDTAC system. Here we can perform functions like, create policies, deploy policies.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

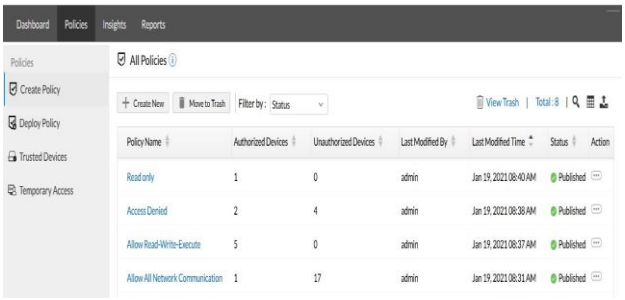

Figure 4: Dashboard Set of policies

We can check trusted devices with its device type and access permission as shown in figure 5.

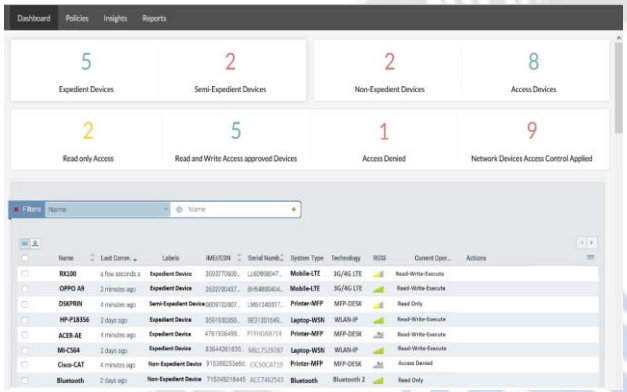

Figure 5: Log of Devices with its access permission and device type

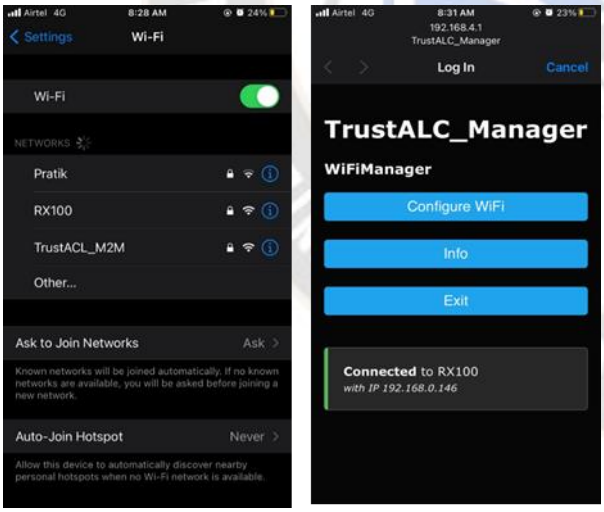

Figure 6 : DDTAC on NodeMCU

In this paper to evaluate and test the developed DDTAC we designed the complete application and ACL which can be deployed on any network devices which having capacity to reconfigure or reprogram its basic functional model. To start with we considered this deployment on the NodeMCU as shown in figure 6. This is the Microcontroller development board having capacity to reprogram its base functional model with ability to communicate on Wireless network using WiFi 802.11 technology.

Proposed Access control is configured and implemented on NodeMCU and can be accessed via any wireless network enabled device. Figure 7 shows Screenshot of Configuring devices in network.

Figure 8 shows the devices list with attributes which can be taken into consideration for device classification.

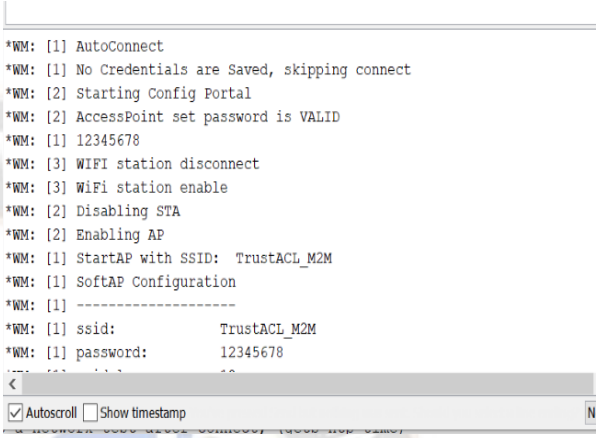

Figure 7 : Screenshot of Configuring devices in network

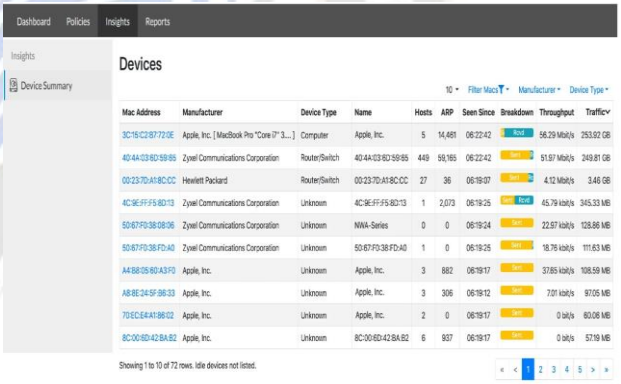

Figure 8: Device list

Figure 9, Represents the device classification based on the parameters into category of Expedient, Semi-Expedient and Non-Expedient. Along with Trust Factor calculation and categorization into Low, Medium and High trust. For further evaluation and DDTAC based control over network connection and communication.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

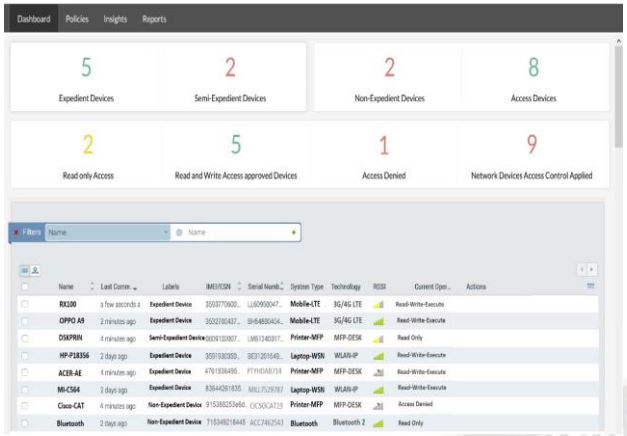

Figure 9: Device Classification

6. RESULT AND DISCUSSION

Performance evaluation of the DDTAC system is performed using Network Simulator (NS2). NS2 simulator is executed on LAPTOP-0237KJUA and processor is Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz 1.19 GHz, Installed RAMis 4.00 GB. ns-allinone-2.34 package tool has used to evaluate DDTAC protocol. Simulation parameters are mentioned in table 2.

TABLE 2 SIMULATION PARAMETER

Simulation Network Area	500m x 500m
Number of nodes	100 to 700
Total Simulation Time	1000s
Value of Initial Energy	100J
Transmission Power	0.06mW
Receiving Power	0.03mW
Application start time	35s
Application stop time	190s
Number of Attackers	3,6,9,12,15
Packet Size	64 bytes
Data Interval	0.1s

Performance metrics:

A. Time Delay in device connection:

It is time required to connect device in network. Table 3 presents the detailed time delay during the execution time of the TAACS, RBAC, DACIoT and DDTAC system. Table 3 and figure 10 shows the average delay in set of concurrent connection happened during the simulation and testing of the DDTAC. TAACS, RBAC, DACIoT are also simulated under similar parameters. Trust is already calculated so less time required to connect device in network in DDTAC scheme. As connection time is less it is useful for time-aware applications and critical use cases.

TABLE 3: TIME DELAY IN DEVICE CONNECTION

Nodes	RBAC[9]	DACIoT [7]	TAACS [3]	DDTAC
100	13.54798	5.00896	8.04798	0.7583548
200	13.87364	5.40896	9.71536	0.7749344
300	13.89364	9.60449	11.81537	0.9144673
450	14.44788	9.90592	13.19365	0.8500726
500	14.44788	9.60999	13.18352	0.8735712
550	14.34651	9.60999	14.19274	1.08849916
600	14.34651	10.00823	15.85173	1.0958896
650	15.61935	10.00823	15.32729	1.1615931
700	15.81536	10.00937	15.72948	1.1726412

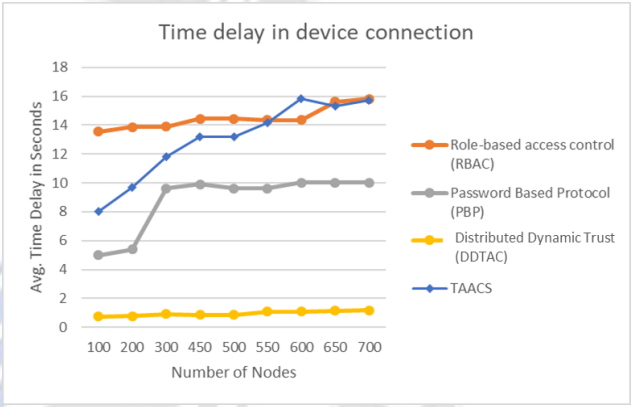

Figure 10: Time Delay in device connection.

After devices get connected in network, the DDTAC performs the process of calculating trust factor and storing it into non-volatile memory for each as Low, Medium and High. Further DDTAC performs the Device classification and put devices in the class of Expedient, Semi-expedient and Non-Expedient for performing access controlled based access to network.

B. Throughput of the 30 concurrent real time devices on Network:

Table 4 and Figure represent, the throughput of the system. Test environment created to test the deployed systems architecture and performance in real time with 30 device concurrent connections, the average time for each phase to proceed is mentioned in the table and it shows good performance in compare to other existing Access Controls examined and tested before implementing DDTAC. Number of Devices mentioned in table 4 are real time devices where Trust score is High. As number of devices increases there is negligible change in throughput. So, it shows that DDTAC system achieved scalability.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

TABLE 4 THROUGHPUT OF THE 30 CONCURRENT DEVICES ON NETWORK

Device No	Trust Calculation Time	DID and Encryption time	ACL offered time	Devices on network	**Total Time**
1 ≥ 5	4.29	5.18	4.16	1.16	**14.79**
1 ≥ 15	5.01	6.12	5.78	2.06	**18.97**
1 ≥ 20	5.09	6.18	5.08	2.46	**18.81**
1 ≥ 25	6.05	6.81	5.02	3.02	**20.9**
1 ≥ 30	7.29	7.45	6.23	3.63	**24.6**

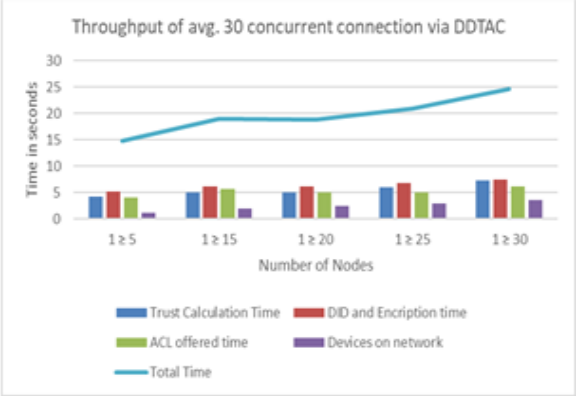

Figure 11: Throughput of the 30 concurrent devices on Network

C. Attack Resistance: MiTM, Sniffing, Session Hijacking:

The model is considered as light weight Access control model and can be deployed on any network reprogrammable devices such as NodeMCU in our testing conditions. It is being observed and test that average time system takes to implement to DDTAC is also affected during any logical attacks to bypass the system. In developed real-time testing environment, the developed system is checked against the Man-in-the-Middle attack, Sniffing attack, Session Hijacking attacks and Injection attacks.

Table 5 and figure 12 shows the average time (in sec) takes by the system to resist the attack and alert for the same and all of the results were indicated the adequate attack resistance capacity is implemented due to a DID, strong encryption and Trust Factor calculation schema. To check security and protocol analysis, we have used EtterCap tool to create MiTM attack, Session Hijacking Attack, Sniffing and Injection Attacks. This tool return request and response time. Based on these values we got time to resist attack. According to result there is negligible change in time as number of devices increases. So, it shows that system is lightweight and scalable.

TABLE 5: DDTAC ATTACK RESISTANCE CAPACITY IN SECONDS

Device No	**MiTM Attack**	**Sniffing**	**Session Hijacking**	**Injection attacks**
1 ≥ 5	4.29	5.18	4.72	1.81
1 ≥ 15	7.29	7.18	5.93	2.63
1 ≥ 20	10.29	9.18	6.43	3.99
1 ≥ 25	13.29	11.18	7.71	4.16
1 ≥ 30	16.29	13.18	8.42	5.54

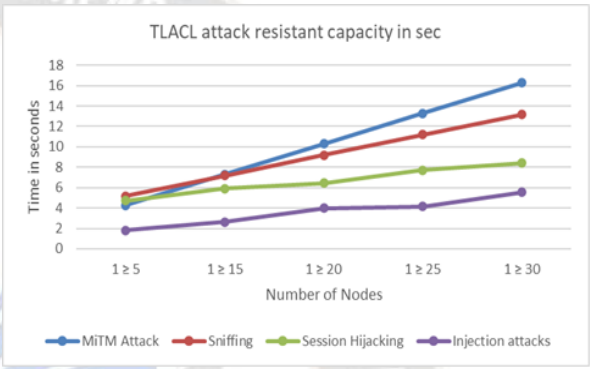

Figure 12: DDTAC Attack resistance capacity in seconds

7. FORMAL SECURITY ANALYSIS

Proposed protocol formally checked on EtterCap tool. This tool uses unified sniffing method which is base for attack [20],[21] Man in middle attack can be Sniffing attack, Session Hijacking attacks and Injection attacks. Before getting access to resources, attacker should authenticate by authentication system, if attacker success to bypass authentication system, then DDTAC system which is tightly coupled on Node MCU checks for its device type, trust score and access permission of attacker's device. DDTAC secured by trusted platform module leveraging functionality of embedded security. If attacker accessing DDTAC first time, trust score of this attacker device is neutral. As per policies written for neutral device is read only permission, but data is encrypted with its keys which generate using DIDs. All verifiable credentials required for DID are hidden [19] that's why attacker is not able to read encrypted data. EECDH [22] [23] scheme used to protect data from MiMTM attack, Sniffing attack, and Session Hijacking attacks. A sample sequence diagram for MiMTM attack, sniffing attack, and Session Hijacking attacks is shown in figure 13.

As, there will be no successful communication between devices trust score get reduced. For low trust devices there will not be permission to read data, so for attacker permission will be access denied [6]. In this way our system mitigates unauthorized access.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

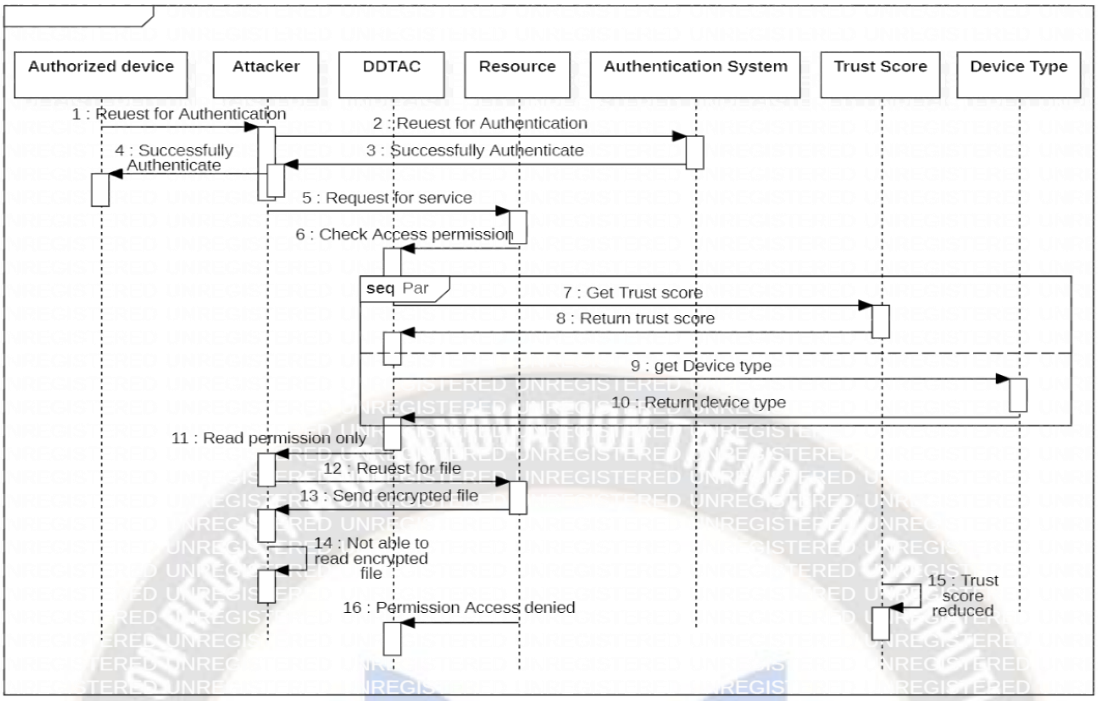

Figure 13: DDTAC Attack resistant sequence diagram

8. Conclusion And Future Work

Security is prime concern in IoT network for machine-to-machine communication. To provide proper access to trusted devices in distributed environment is very crucial task. This paper proposes dynamic access control in distributed environment based on trust score and device classification. This DDTAC framework support selective disclosure and principle of leas privileges. Decentralized Identifiers and Verifiable Credentials are used to provide selective disclosure and privacy preserving in this framework. DDTAC protocol is implemented, tested and checked performance analysis against with existing Access control protocol and it proves that it required less time to connect device in network. As number of devices increases there is negligible change in throughput. So, it shows that DDTAC system achieve scalability. DDTAC is attack resistant to Man-in-the-Middle attack, Sniffing attack, Session Hijacking attacks and Injection attacks. Our goal of this paper is to proposes dynamic access control in distributed environment and we have achieved it with good performance for this scheme. In the future, our planning is to explore the security of our connected devices for real time use cases.

References

[1]. Kevin Ashton, "That 'Internet of Things' Thing", RFID Journal, 22 June 2009.

[2]. ITU, TELECOMMUNICATION STANDARDIZATION SECTOR OF. "Overview of the Internet of Things." Recommendation ITU-T Y 2060 (2012): 22.

[3]. Thirukkumaran, R., and P. Muthukannan. "TAACS-FL: trust aware access control system using fuzzy logic for internet of things." International Journal of Internet Technology and Secured Transactions 9, no. 1-2 (2019): 201-220.

[4]. Railkar, Poonam N., Parikshit N. Mahalle, and Gitanjali R. Shinde. "Access control schemes for machine to machine communication in IoT: comparative analysis and discussion." In 2018 IEEE global conference on wireless computing and networking (GCWCN), pp. 59-63. IEEE, 2018.

[5]. Qiu, Jing, Zhihong Tian, Chunlai Du, Qi Zuo, Shen Su, and Binxing Fang. "A survey on access control in the age of internet of things." IEEE Internet of Things Journal 7, no. 6 (2020): 4682-4696.

[6]. Railkar, Poonam Ninad, Parikshit Narendra Mahalle, and Gitanjali Rahul Shinde. "Scalable Trust Management model for Machine To Machine communication in Internet of Things using Fuzzy approach." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 6 (2021): 2483-2495.

[7]. Alkhresheh, Ashraf, Khalid Elgazzar, and Hossam S. Hassanein. "DACIoT: Dynamic Access Control Framework for IoT Deployments." IEEE Internet of Things Journal 7, no. 12 (2020): 11401-11419.

[8]. Ding, Sheng, Jin Cao, Chen Li, Kai Fan, and Hui Li. "A novel attribute-based access control scheme using blockchain for IoT." IEEE Access 7 (2019): 38431-38441.

[9]. Zhang, Guoping, and Jiazheng Tian. "An extended role based access control model for the Internet of Things." In 2010 International Conference on Information, Networking and Automation (ICINA), vol. 1, pp. V1-319. IEEE, 2010.

[10]. Jindou, Jia, Qiu Xiaofeng, and Cheng Cheng. "Access control method for web of things based on role and sns." In 2012

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

IEEE 12th International Conference on Computer and Information Technology, pp. 316-321. IEEE, 2012.

[11]. Ye, Ning, Yan Zhu, Ru-chuan Wang, Reza Malekian, and Qiao-min Lin. "An efficient authentication and access control scheme for perception layer of internet of things." (2014).

[12]. Guoping, Zhang, and Gong Wentao. "The research of access control based on UCON in the internet of things." Journal of Software 6, no. 4 (2011): 724-731.

[13]. Hernández-Ramos, José L., Antonio J. Jara, Leandro Marín, and Antonio F. Skarmeta Gómez. "DCapBAC: embedding authorization logic into smart things through ECC optimizations." International Journal of Computer Mathematics 93, no. 2 (2016): 345-366.

[14]. Mahalle, Parikshit N., Pravin A. Thakre, Neeli Rashmi Prasad, and Ramjee Prasad. "A fuzzy approach to trust based access control in internet of things." In Wireless VITAE 2013, pp. 1-5. IEEE, 2013.

[15]. Almenárez, Florina, Andrés Marín, Celeste Campo, and Carlos García. "TrustAC: Trust-based access control for pervasive devices." In International Conference on Security in Pervasive Computing, pp. 225-238. Springer, Berlin, Heidelberg, 2005.

[16]. Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, "Identity driven Capability based Access Control (lCAC) for the Internet of Things," In 6th IEEE International Conference on Advanced Networks and Telecommunications Systems (IEEE ANTS 2012). Bangalore – India, December 16-19 2012.

[17]. Anggorojati, Bayu, Parikshit Narendra Mahalle, Neeli Rashmi Prasad, and Ramjee Prasad. "Capability-based access control delegation model on the federated IoT network." In The 15th International Symposium on Wireless Personal Multimedia Communications, pp. 604-608. IEEE, 2012.

[18]. Buschsieweke, Marian, and Mesut Güneş. "Securing critical infrastructure in smart cities: Providing scalable access control for constrained devices." In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-6. IEEE, 2017.

[19]. Kortesniemi, Yki, Dmitrij Lagutin, Tommi Elo, and Nikos Fotiou. "Improving the privacy of iot with decentralised identifiers (dids)." Journal of Computer Networks and Communications 2019 (2019).

[20]. Norton, Duane. "An ettercap primer." SANS Institute InfoSec Reading Room 5 (2004).

[21]. https://www.ettercap-project.org/

[22]. Anand, Shajina, and Varalakshmi Perumal. "EECDH to prevent MITM attack in cloud computing." Digital Communications and Networks 5, no. 4 (2019): 276-287.

Poonam N. Railkar: Dr. Poonam N. Railkar received PhD degree from SPPU University Pune in the year 2022. She completed her Master in Computer Engineering (Computer Networks) from Pune University Maharashtra, India in the year 2013. From September 2012 working as an Assistant Professor in Department of Computer Engineering, STES's Smt. Kashibai Navale College of Engineering, Pune, India. She has published 20 plus papers at national and international journals and conferences and authored 1 book. She has guided more than 20 plus under-graduate students and 3 plus postgraduate students for projects. Her research interests are Internet of Things, Identity Management, Security and Database Management System Applications.

Dr Parikshit is a senior member IEEE and is Professor and Head of Department of Artificial Intelligence and Data Science at Vishwakarma Institute of Information Technology, Pune, India. He completed his Ph. D from Aalborg University, Denmark and continued as Post Doc Researcher at CMI, Copenhagen, Denmark. He has **22 + years** of teaching and research experience. He is a member of the Board of Studies in Computer Engineering, Ex-Chairman Information Technology, SPPU and various Universities and autonomous colleges across India. He has 9 patents, 200+ research publications **(Google Scholar citations-2179 plus, H index-22 and Scopus Citations are 1100 plus with H index -15)** and authored/edited 40+ books with **Springer, CRC Press, Cambridge University Press,** etc. He is editor in chief for IGI Global –International Journal of Rough Sets and Data Analysis, Associate Editor for IGI Global - International Journal of Synthetic Emotions, Inter-science International Journal of Grid and Utility Computing, member-Editorial Review Board for IGI Global – International Journal of Ambient Computing and Intelligence. His research interests are Machine Learning, Data Science, Algorithms, Internet of Things, Identity Management and Security. He is a recognized PhD guide of SSPU, Pune, and guiding 7 PhD students in the area of IoT and machine learning. Recently, **FIVE** students have successfully defended their PhD. He is also the recipient of "Best Faculty Award" by Sinhgad Institutes and Cognizant Technologies Solutions. He has delivered 200 plus lectures at national and international level. He is also the recipient of the best faculty award by Cognizant Technology Solutions

Gitanjali Shinde: Dr. Gitanjali Rahul Shinde has obtained his B.E degree in Computer Engineering from Savitribai Phule Pune University, Pune, India and M.E. degree in Computer Engineering from Savitribai Phule Pune University, Pune, India. She completed her PhD from Aalborg University Denmark. From September 2008, she is currently working as an Assistant Professor in Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India. She has published 40 plus papers at national and international journals and conferences. She has guided more than

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5820
***Article Received**: 24 August 2022 **Revised**: 29 October 2022 **Accepted**: 22 November 2022*

25 plus under-graduate students and 7 plus postgraduate students for projects. Her research interests are Internet of Things, System Programming, Operating System, Theory of computation and Wireless Communication.

Dr. Nilesh P. Sable has overall 14 years of experience, presently working as SPPU Approved Associate Professor in the Department of Information Technology, Vishwakarma Institute of Information Technology, Pune, India. He has done a Ph.D. in Computer Science & Engineering from Kalinga University, Raipur on Research Problem Statement "STUDY ON RELATIONSHIP STANDARD MINING CALCULATIONS IN DATA MINING" – Ph. D awarded on 3rd June 2018. He obtained M.Tech. (Information Technology) degree from JNTU, Hyderabad in 2014 and a B.E. (Information Technology) degree from the University of Pune, Pune in 2008. He is SPPU Approved Ph.D. Research Guide. He has published 40+ papers in National, International conferences and journals. He had Filed and Published 10+ Patents and Copyrights. He is the author of a couple of books with an international publisher like Lambart.