ijar
ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/3724
DOI URL: http://dx.doi.org/10.21474/IJAR01/3724

RESEARCH ARTICLE

A CERTIFICATE-DRIVEN APPROACH TO ACCESS CONTROL IN FUTURE INTERNET.

Nancy Ambritta P[1]., Poonam N. Railkar[2] and Parikshit N. Mahalle[2].

1. Sinhgad Institute Of Technology And Sciences, Savitribai Phule Pune University, Pune, India.
2. Smt. Kashibai Navale College Of Engineering, Savitribai Phule Pune University, Pune, India.

Manuscript Info

Manuscript History

Received: 15 January 2017
Final Accepted: 10 February 2017
Published: March 2017

Key words:-
Future Internet, mutual authentication, collusion attack, privacy, content integrity, normal distribution, bell curve, recurrence relation, time complexity

Abstract

The growing impact of the Internet in all walks of human life has also introduced us to newer problems related to security and hence the increasing demands to address such threats that prevail. The Future Internet (FI) being a confluence of various technologies, and the cloud being one such component technology in the FI that provides storage as a prominent service amongst the other services offered by it, it follows that the public cloud cannot be trusted at all times and therefore cannot be completely relied upon to regulate access to the stored sensitive data that it contains. This creates an avenue for collusion attack by the cloud and a malicious user. This has been addressed in our proposed system by the separation of access policy and access structure. Further considering the insecure communications and the vulnerability of the transmitted data, a mutual identity establishment scheme has been proposed to secure the channel and therefore the contents in transit. A recurrence relation for the established scheme has been derived to calculate its time complexity and the time taken to achieve mutual authentication has been administered for repeated iterations and the values thus obtained have been plotted and verified under the normal distribution bell curve to suggest the model's consistency and adaptability.

Introduction:-

Internet has become an essential technology that impacts billions of people in every aspect of our lives today. Internet of today has billions of connected devices which are still predicted to evolve/increase over the years to come. It is facing multidimensional challenges ranging from attacks to performance issues, while at the same time should never cease upon its responsibility of maintaining organizations' and personal integrity and privacy. Hence there are ever increasing research activities in progress on having the Future Internet (FI) to address its current shortcomings. The future Internet being a confluence of devices, technologies and areas, and access management being one such area of concern in association with its component technology the FI, an attempt has been made in this paper to address a few security issues namely, collusion attack, replay attack resistance, mutual authentication establishment and content integrity.

Motivation:-

The evolution of Internet and its advancements that press towards the establishment of a futuristic era that involves a confluence of various devices/things intermittently connected online to exchange data/information and provide

Corresponding Author:- Nancy Ambritta P.
Address:- Sinhgad Institute Of Technology And Sciences, Savitribai Phule Pune University, Pune, India.

services, has led to the growth of demands in terms of security, privacy and trust which are the basic elements that need to be satisfied from an end user's point of view. The lack of a proper authentication mechanism and secured ways of exchanging data makes it easier for an intruder to steal/sniff data illegally thereby affecting the security and privacy of the users. Also, considering the usage of a public cloud, the cloud cannot be trusted all the time, and hence is capable of exposing sensitive data maliciously (collusion attack). This necessitates us to develop suitable architectures and algorithms that helps address the security, authentication (for secure channel establishment) and content integrity issues that occur in a communication between participating entities.

Related work and evaluation:-

Table 1:- Related work and Evaluation

Paper No	Mutual Authentication	Content Integrity	Forward Secrecy maintenance	Trust
[4]	No-one way	Not addressed	Not addressed	One way (server is assured trust on the requesting device)
[5]	No-one way	Not addressed	Not addressed	Not addressed
[6]	No-one way	Yes-hiding of data using one way hash function	Yes- session parameters and pseudorandom numbers	One way (server is assumed to trust on the requesting device)
[7]	No-one way	Not addressed	Not addressed	Authorization function delegated to third party, requires an assumed trust level.
[8]	Yes-Chbyshev chaotic maps	Yes – aggregated proofs	Yes- session parameters and pseudorandom numbers	Yes
[9]	No-one way	Partial – privacy on data stored not on user private information	Not addressed	Yes, Trusted third party
[10]	No-one way	Yes , OAuth	Not addressed	Pre-requisite for authentication

The need to regulate access to critical and sensitive information has led to the proposal of numerous access control schemes like the Dynamic broadcast encryption technique [1], role based access control (RBAC) [2] and Attribute based encryption (ABE) [3] which have addressed the issues such as scalability and anonymity. However, the assumption that the cloud is honest (trusted) but curious, does not hold good at all times since the cloud, controlled by the cloud service provider (CSP) may not belong within the trusted domain of the involved association/group thereby providing greater avenue for the cloud to expose the access policy (rules that regulate access to the sensitive data and provides protection) to malicious attackers and collude with them posing threat to the stored sensitive data.

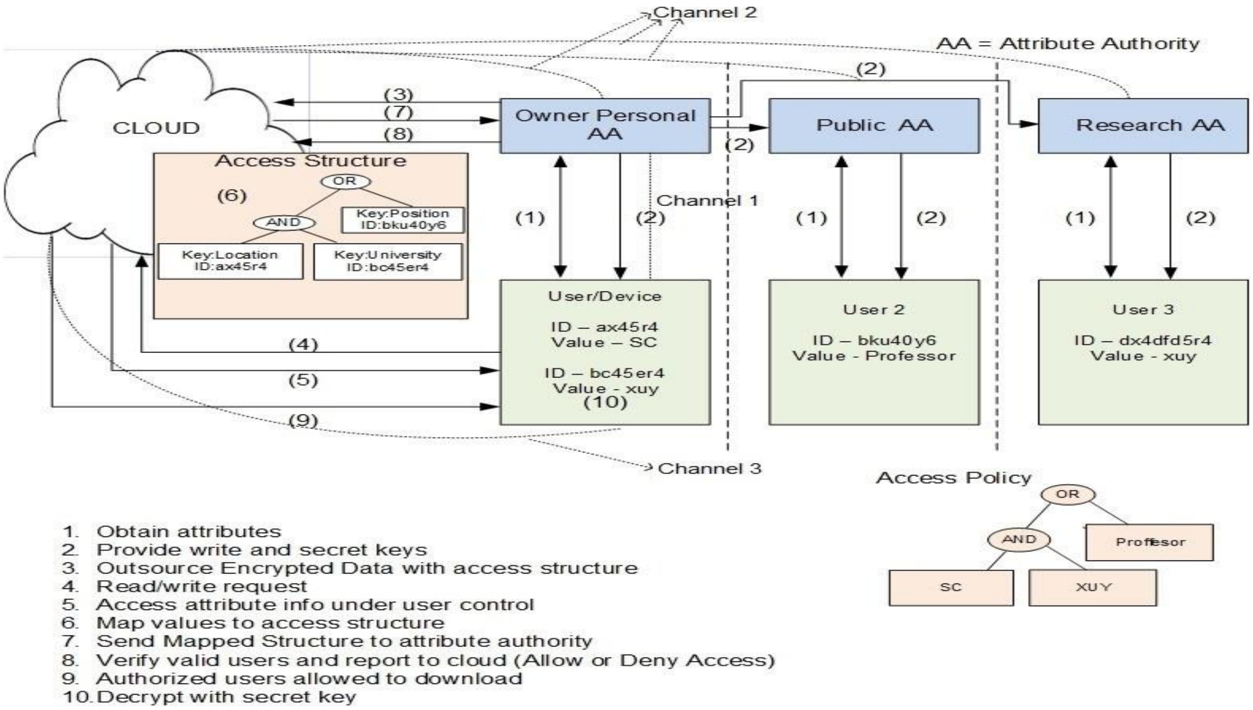
Even though SLAs address this as a legal issue, preventing such attacks by providing technical solutions makes the system resilient and more reliable. Also, several schemes have beenintroduced to address the security issues that prevail in the various areas that make up the Future Internet. A few solutions include the challenge-response protocol coupled with a novel two factor authentication protocol [4], Kurento and Nubomedia [5], a Shared Authority based Privacy Preserving Authentication protocol (SAPA) to address the privacy issues using the Attribute based Access Control (ABAC) and proxy re-encryption scheme [6], a HTTP/CoAP (Constrained Application Protocol) service based architecture to provide an authorization framework [7], an aggregated proof based Hierarchical Authorization scheme in U2IoT [8], a novel privacy preserving authenticated Access Control scheme [9] and an optimization work on the OAuth 2.0 protocol [10] to solve the associated performance challenges while still ensuring privacy of user sensitive credentials.

However in all such cases the necessity to establish a trusted communication channel via mutual authentication and ensuring the integrity of the user sensitive data that is exchanged between devices has not been considered. Also, forward secrecy, a phenomenon wherein an attacker should be incapable of tracing back to the data transmitted previously with the information that he has managed to fetch at that instance is not considered in most cases. Table 1 summarizes the above discussions and provides a comparative analysis of a few security issues discussed in this section.

Proposed Architecture:-

Fig 1 shows the proposed architecture [11] that addresses the security issues such as maintaining user privacy (by providing a user controlled environment) and collusion attack caused due to the exposure of access policy that contains the sensitive user information to the cloud. The sequence of steps that occur in the system are labeled [1-10] in the figure below. As shown in fig 1. The system consists of three entities namely the Attribute Authority ((AA) owner of the data), the public cloud that provides services in terms of storage and processing power, and the users/devices with their sensors. The communication between the entities follows a model wherein the access policy lies with the sole owner AA and the AAs within the trusted domain of the owner.

The AA requires that the cloud and the devices register themselves initially depicted as channel 1 in fig 1. The AA provides certificates to the entities upon registration, which is to be used later to prove their identities to establish trust amongst the participating entities.The AA uploads the encrypted data and documents along with the access structure to the public cloud. The cloud only possesses the access structure (contains key and ID of values in the access policy) that facilitates it to map the user/device attribute values by matching the associated IDs of attributes. The cloud is therefore left unclear about the actual attribute values that facilitate access to the data. Its job is therefore limited to storing the data and collecting the required attributes, and forwarding it to the appropriate AA whichultimately makes the decision about allowing/denying access after comparison with the respective access policy. The cloud is thereby prevented from participating and executing a collusion attack.



1. Obtain attributes
2. Provide write and secret keys
3. Outsource Encrypted Data with access structure
4. Read/write request
5. Access attribute info under user control
6. Map values to access structure
7. Send Mapped Structure to attribute authority
8. Verify valid users and report to cloud (Allow or Deny Access)
9. Authorized users allowed to download
10. Decrypt with secret key

Fig 1:- Proposed Architecture

Algorithmic Details:-

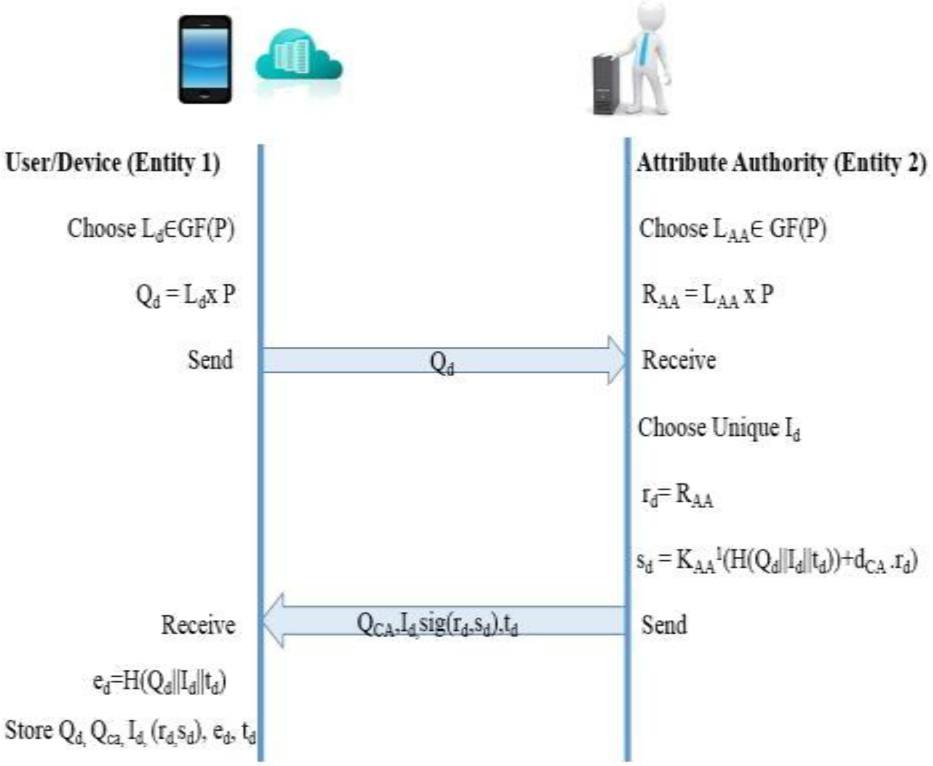

User/Device (Entity 1)
Attribute Authority (Entity 2)
Choose $L_d \in GF(P)$
Choose $L_{AA} \in GF(P)$
$Q_d = L_d x P$
$R_{AA} = L_{AA} x P$
Send
Q_d
Receive
Choose Unique I_d
$r_d = R_{AA}$
$s_d = K_{AA}^{1}(H(Q_d||I_d||t_d))+d_{CA}.r_d)$
Receive
$Q_{CA}.I_d sig(r_d.s_d).t_d$
Send
$e_d=H(Q_d||I_d||t_d)$
Store $Q_d, Q_{ca}, I_d, (r_d s_d), e_d, t_d$

Fig2:- Certificate Distribution.

The communication between the entities namely the AA, user/device and cloud are classified into three parts namely,

1. AA (server) ->User/device/cloud (client) [user/devices register with the AA and obtain keys] represented as channel 1a and 1b in fig 2.
2. Cloud (server) <-> user/device (client) [user/devices request access to data on the cloud] represented as channel 2 in fig 2.
3. AA (server) <-> Cloud (client) [cloud sends the collected and mapped data for verification to the AA] represented as channel 3 in fig 2 [12][13].

In all the above cases the proposed mutual identity establishment scheme is executed in order to ensure the establishment of a secure communication channel and integrity of transmitted message. This scheme adopts the ECCDH (Elliptical curve diffie Hellman) mechanism for the establishment of a shared secret key (Qsk) between the participating entities shown in fig 2. The execution of the scheme is threefold. First, as mentioned earlier, the AA issues certificates to the devices and cloud shown in fig 2.This certificate consists of a unique temporary ID (I_d) chosen by the AA for the cloud/device which in turn performs a hash on the chosen Identity and the certificate expiration time, signs it and passes it over to the cloud/device which is then utilized for authentication.

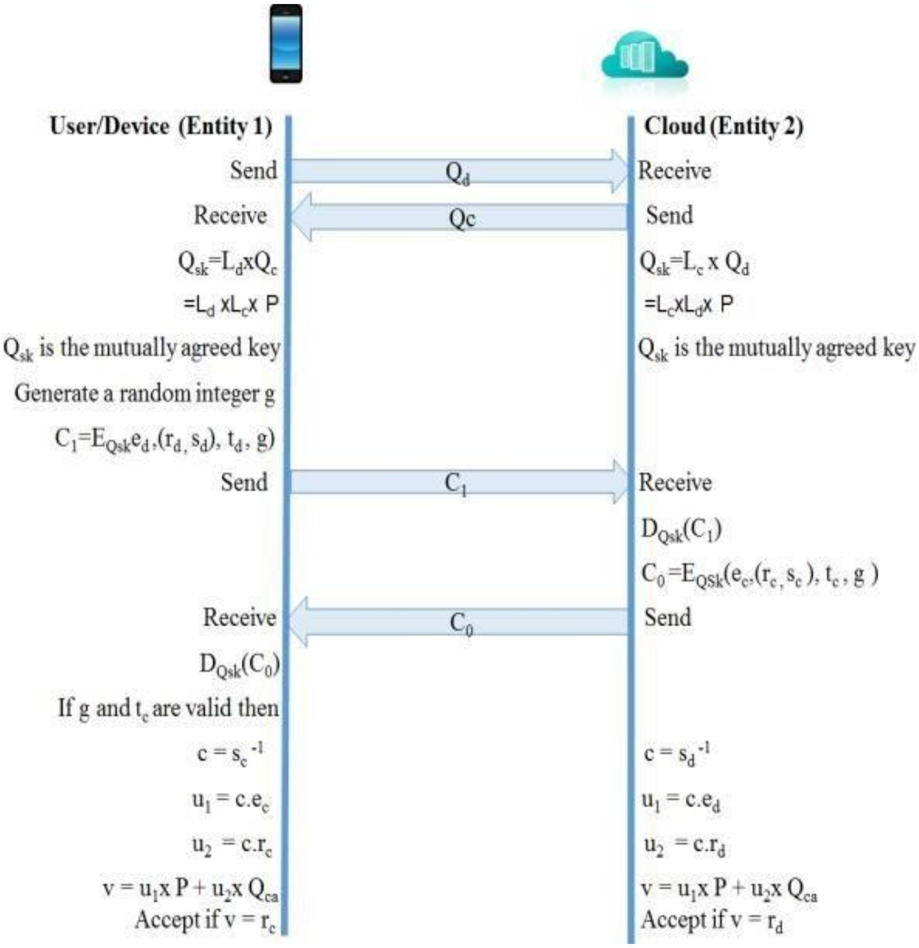


Fig 3:- Mutual authentication

Further, in order to ensure the establishment of a secure channel for exchange of data, mutual authentication has been implemented via exchange of the participating entities' certificates and a random number g that is appended to the certificate and encrypted with the shared secret key obtained via ECCDH to maintain the freshness of the exchanged information. The certificates are then verified on either side following theECCDSA's (Elliptical curve Cryptography Digital Signature Algorithm) verification mechanism.This establishment of mutual authentication provides a secured communication channel to ensure trust, and prevents the privacy theft/tampering of the exchanged information (user attributes/requests and request approval from AA).

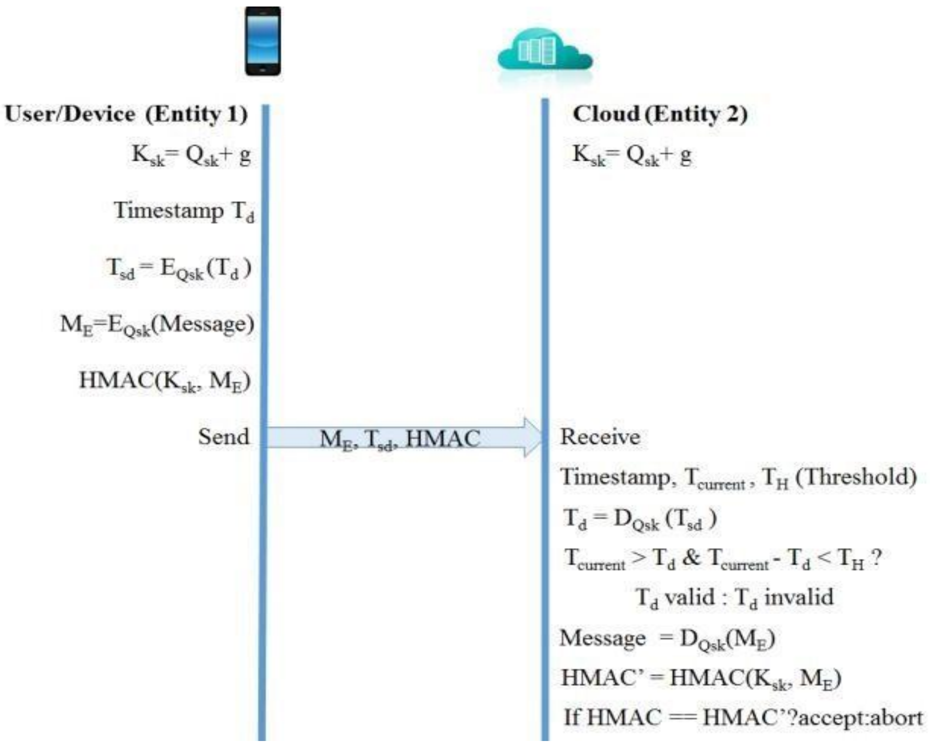

User/Device (Entity 1)
$K_{sk} = Q_{sk} + g$
Timestamp T_d
$T_{sd} = E_{Qsk}(T_d)$
$M_E = E_{Qsk}(\text{Message})$
$\text{HMAC}(K_{sk}, M_E)$
Send
M_E, T_{sd}, HMAC
Cloud (Entity 2)
$K_{sk} = Q_{sk} + g$
Receive
Timestamp, $T_{current}$, T_H (Threshold)
$T_d = D_{Qsk}(T_{sd})$
$T_{current} > T_d$ & $T_{current} - T_d < T_H$?
T_d valid : T_d invalid
Message $= D_{Qsk}(M_E)$
$\text{HMAC}' = \text{HMAC}(K_{sk}, M_E)$
If HMAC == HMAC'?accept:abort

Fig 4:- Content Integrity

Also, the integrity of the transmitted message is achieved by computing a HMAC of the encrypted message (ME,encrypted by using the shared secret key (Qsk)) and the attribute structure is flushed off from the cloud by using the session management techniques, transported to the other side where the encrypted value of timestamp is decrypted and verified against a predefined threshold time (TH) thereby enabling the detection of replay attack. A session key Ksk is generated by adding the random number g with the shared secret key to help maintain sessions by which we can ensure that the mapped attributes are not retained at the cloud after transfer to the AA. This shared secret key is used to compute the HMAC of the encrypted message ME.

The computed HMAC, encrypted time-stamp (using shared secret key (Qsk)) and encrypted message (ME) are transmitted to receiver (Entity2) and any attacks/tampering of data is identified by verifying the received HMAC against the recomputed HMAC' on the receiver (Entity2) side. If any discrepancy is detected the received content is discarded, otherwise accepted for further processing. Fig 3 shows the mutual authentication establishment scheme for the communication between a device and the cloud and fig 4 shows the content integrity maintenance scheme in the communication between a device and the cloud.

A similar scheme that follows the same sequence of operations is defined for the communication between the cloud (client) and the AA (server) to achieve mutual authentication and content integrity.

Time Complexity Analysis and Performance Evaluation of the System:-

A recurrence relation for the proposed mutual identity establishment scheme presented in the previous section is given below as

$T(n) = a\,T(n / a) + 3n$ Where, n represents the number of requests that are incident at the cloud/AA/server via any device/user (client).

a, represents the number of domain attribute authorities(AA) which in the proposed system amounts to three AAs . Here the requests that arrive at the cloud are assigned to the appropriate attribute authorities which is given by n/a or n/3 and is handled by each of the AAs individually at each domain, therefore multiplied by the total number of attribute authorities i.e., aT(n/a) or 3T(n/3)).

3n, is a summation of the time required to distribute certificates for n entities that register with the AA (n units of time), time required to establish mutual authentication for n entities/devices and their associatedrequests (n units of time)Upon solving the recurrence relation by master's theorem to obtain the running time complexity we get,

Iteration frequency	2	1	2	3	4	1	1	2	1	1	1	2	2	1	2	1	1	1	1	1
MA in ms	410	422	450	470	440	423	467	455	434	450	447	420	445	442	430	432	433	460	483	462

Table 2:- Mutual Authentication (MA) Time Dataset in Milliseconds.

T(n) =O(nlogn) [since =n and f(n) = 3n ≈ n upon ignoring the constant term associated with n] and time required for integrity check of the transmitted contents (n units of time).

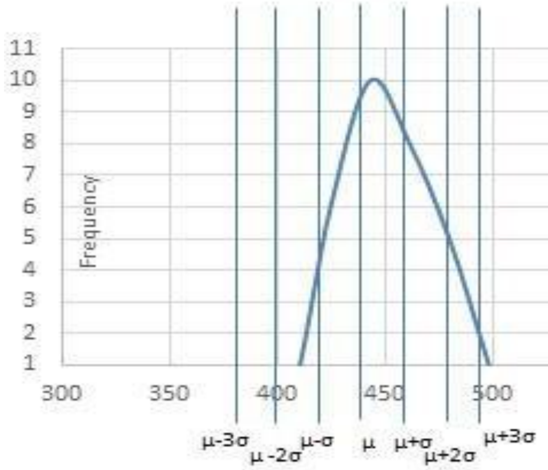


Fig 4:- Content Integrity

Further, the implementation of the proposed algorithm in the system has been verified against 30 iterations and the amount of time taken to mutually authenticate the devices was noted. For the data given in table 2 we calculate the average to be 443.1667ms and standard Deviation 18.41753. In statistics, the so-called 68– 95–99.7 rule indicates the percentage of values that lie within a band around the mean in a normal distribution with a width of one, two and three standard deviations, respectively. With our data set of 30 samples we find that all the values fall within the width of three standard deviations i.e. 99.73% as depicted in the bell curve in fig 5, which suggests that the proposed model is predictable with no outliers and ideal for use.

Conclusion and Future Work

This paper has established the need for Future Internet to address privacy and integrity of exchanges/transmitted data that will determine its successful adoption universally. It has provided an insight into the proposed system and its resistance to collusion attack. Also, the reader has been introduced to the mutual identity establishment scheme that ensures secure transfer of data through the establishment of a secure channel via mutual authentication establishment and assurance of content integrity. We have successfully derived a recurrence relation for the proposed scheme and calculated the running time complexity for the same. Also, a plot (normal distribution bell curve) of the different times taken for mutual authentication for numerous iterations has revealed the system's consistency in performance and its adaptability. In future we propose to extend the scheme to implement the auto-delegation mechanism along with the interoperability of the devised protocol with the existing ones.

References:-

1. Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, 'Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud', IEEE Transactions On Parallel and Distributed Systems,Vol. 24, No. 6, June 2013.
2. M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in Proc. IEEE INFOCOM, May 2007, pp. 1307-1315.Lan Zhou, Vijay Varadharajan, and Michael Hitchens, AchievingSecure Role-Based Access Control on Encrypted Data in Cloud Storage,IEEE Transactions On InformationForensics and Security, Vol. 8, No.12, December 2013.
3. Kan Yang, XiaohuaJia, KuiRen, Bo Zhang andRuitaoXie, DACMACS: Effective DataAccessControl for Multiauthority Cloud Storage Systems, IEEE TransactionsOn Information Forensics And Security, Vol. 8, No.11, November 2013.
4. Aldar C.-F. Chan, and JianyingZhou,CyberPhysical Device Authentication for the Smart Grid Electric Vehicle Ecosystem,IEEEJournal on selected areas in communications, Vol.32, No. 7, JULY 2014
5. David Fernndez-Lpez and Francisco Javier Lpez,Authentication, Authorization, and Accounting in WebRTCPaaSInfrastructures,IEEEInternet Computing,pp: 34-40,Issue No.06,vol.18, Nov-Dec 2014
6. Hong Liu, HuanshengNing, QuigxuXiong, Lawrence T. Yang,Share Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing, IEEE Transactions On Parallel and Distributed Systems, Vol 26, No. 1, January 2015
7. Simone Cirani, Marco Picone, Pietro Gonizzi, Luca Veltri, and GianluigiFerrari,IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoTScenarios,IEEE Sensors Journal, Vol. 15, No. 2, February 2015
8. HuanshengNing, Laurence T. Yang,Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things,IEEETransactions on Parallel and Distributed Systems,Vol. 26, No. 3, March 2015
9. SushmitaRuj, Milos Stojmenovic, Amiya Nayak,Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds,IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014
10. M. Noureddine, R. Bashroush,An Authentication Model towards Cloud Federation in the Enterprise,The Journal of Systems and Software,Volume 86, Issue 9, pp 22692275 September 2013
11. Nancy Ambritta P., Poonam N. Railkar and Parikshit N. Mahalle,Proposed Identity and Access Management in Future Internet (IAMFI): A Behavioral Modeling Approach,Journal of ICT, Vol. 2 1, 136, July, 2014
12. Parikshit N. Mahalle, BayuAnggorojati, Neeli R. Prasad and Ramjee Prasad, Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things,Journal of Cyber Security and Mobility, Vol. 1, 309348, February 2013
13. Nancy Ambritta P., Poonam N. Railkar and ParikshitN. Mahalle ,' Collaborative Mutual Identity Establishment (CMIE) for the Future Internet, IJPCC