ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

National Symposium On Emerging Trends In Computing & Informatics, NSETCI 2016, 12th July 2016, Rajagiri School of Engineering & Technology, Cochin, India.

Secure Authentication Schemes in IoT Environments.

***Sherin Peter[1] and Raju.K.Gopal[2].**

1. Department of Computer Science and Engineering, Mar Baselios College of Engineering & Technology , Trivandrum, India
2. Professor, Department of Computer Science and Engineering, Mar Baselios College of Engineering & Technology, Trivandrum, India

Manuscript Info

Key words:
Internet of Things,
Authentication,
Security

Abstract

With the ready increase in the demand for Internet of Things (IoT) services, securing the information content delivered among various entities involved in the IoT architecture has become an important issue. Accordingly, the problem of Internet of Things security has become more and more challenging day-by-day. In an Internet of Things background a variety of devices and appliances are interconnected and these things can assemble data, communicate and build decisions with or without human interactions. Based on the application necessities in various IoT scenarios different authentication schemes are needed. And these authentication schemes should supply security against the various IoT attacker models. This paper presents general analysis of Internet of Things, its security aspects and comparison among different authentication schemes proposed in the literature to authenticate Internet of Things architectures. Also extend the analysis to authentication techniques for limited energy consuming and resource constrained IoT architectures.

Introduction:-

The Internet has been evolved in 1969. It enabled people to communicate messages, exchange content and provide information. Beyond 2012, it has started the next stage of progression of Internet ie, the "Internet of Things" (IoT). When hidden technology functions behind the scenes and actively responding to how we want things to act, the exact guarantee of IoT is just starting to become aware of. In IoT diverse devices, machines, sensors (Things) are being supplied with Internet connectivity. They can accumulate data, disclose and make decisions with or without human interactions. IoT has excessive possibility to control our environment and consequently affect our lives. As compared to world population the no: of connected devices used by per person increases year by year. Figure 1 shows the hasty increase in connected devices. Thus IoT creates an instructed, invisible network infrastructure that can be sensed, controlled and programmed. Through IoT, thus it allows the Internet to elongate into the authentic world of sensible objects.

As the IoT, is a global Internet-related technical architecture which speed up the exchange of information and benefits; it has an impact on the security and isolation of shared information and services. When interconnected there are dormant vulnerabilities due to the convoluted networks referring to discrepant targets, sensors and backend management systems in IoT. Among the various security measures that can be applied in Iota framework, the authentication has an important role. It is the process for verifying the digital individuality of an entity. In an Internet of Things environment which is an arrangement of physical entities or "things" fixed with software, sensors and electronics; along with the help of existing technologies these machines can collect beneficial information and then

freely flow this between other machines. Based on the application requirements in various IoT scenarios different authentication schemes are needed. And these authentication schemes should provide security against the various IoT attacker models and should provide data confidentiality, forward security, and integrity and privacy preservation.

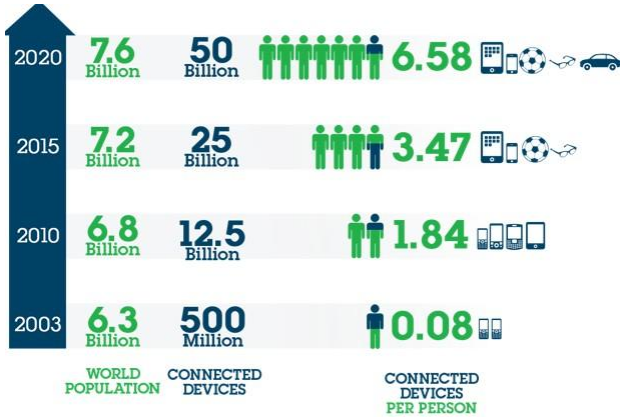


Fig. 1. Increase in Interconnected devices in IoT

Internet of things : vision and security challenges:-

The IoT enables the Internet to spread out into the absolute world enfolding habitual objects. The corporal components are separated from the virtual world no longer, and can execute as physical access points to Internet services and it can be commanded remotely. IoT makes calculation universal In the early 1990s it is bring forward by Mark Weiser initially. This expansion revealed huge scope for both the human being and economy. The perception of IoT is based in the persuasion that the fixed progress which we have observed in recent years in Micro-electronics and the Information technology will continue into the predicted future. It also requires risks and show an extensive skilled and social challenges.

A. IoT Vision Concept:-

The outcome of the name "Internet of Things" (Atzori L and Antonio Iera and Giacomo Morabito., 2010) itself is the logic behind today visible fuzziness about this term, and it is composed of the one drive in the direction of network oriented view of IoT, and the second one moves the target on general "objects" that is to be accommodated into an accepted framework. In the IoT views sometimes differences are considerable which elevate from the truth that professional alliances, experimentation and generalization bodies begin to catch up the issue from any of the "Internet oriented" or a "Things oriented" perspective, that depends on their particular interests, definiteness and circumstances. When put in cooperation, it shall not be let slip from the memory that that the words "Internet" and "Things' accept a meaning that familiarizes a disruptive level of change into world that seen today. The "IoT"semantically defined in such a way that "a network of interconnected things which is world-wide accepted and that are uniquely addressable, located on standard connection protocols". In the process this represents an enormous count of (diversified) objects tangled. The single addressing of object and description and storing of interchanged information be- come the most challenging argument, thus conveys directly to a third, "Semantic oriented", outlook of IoT. The important ideas deals with this are the systems and standards that are featured and classified in remark with the IoT vision/s which they afford for best characterization is shown in Figure. 2. As a result of the convergence of different visions, it shows the Internet of Things paradigm . And from such an analogy, clearly arises that the IoT model is the consequence of the blending of the main three visions addressed above.

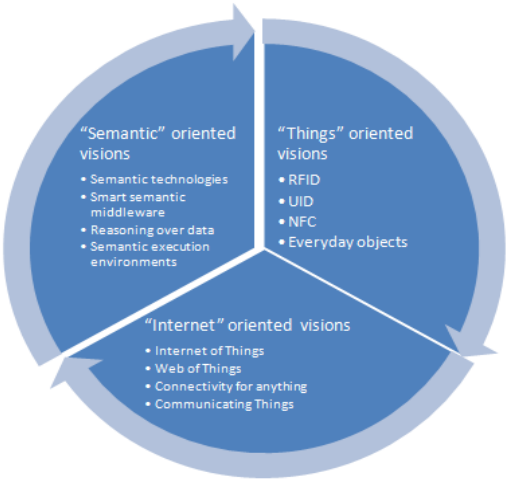


Fig. 2. Internet of Things- Convergence of different visions

The IoT is not developed from a single new technology when considered from a technological point of vision; instead, it involves many of the complementary technical developments that provide facilities which reduces gap in between the implied and corporal world (Friedemann Mattern., 2010) These potentialities comprise:

- ***Identification:-***

The objects should be identifiable uniquely. And the technologies such as RFID, Near Field Communication (NFC) and optically readable bar codes with which the compliant objects can be located that lack built-in energy resources.

- ***Sensing:-***

The information about their neighbouring can be gathered by using the objects equipped with sensors, then document it, after that forward and it can also directly respond.

- ***Actuation:-***

Inorder to employ their environment the objects may have the capacity for being actuators. Using Internet for controlling the real-world actions remotely such motivators can be used.

- ***Embedded information processing:-***

A processor along having storage dimensions represents the smart objects. In order to process and explicate sensor information, these resources can be used or in order to give commodities a "memory" of how working takes place.

- ***Communication and cooperation:-***

To make use of data and update their state, things have the capability to network with Internet resources or even with one another. Wireless methods such as GSM, Zigbee, Wi-Fi, Bluetooth and several other wireless benchmarks currently under making, and in particular the primary importance is to those in relation with Wireless Personal Area Networks (WPANs).

- ***Addressability:-***

The objects can be addressed via exploration within an IoT, the name services can be used, and thus can be isolatable and configured.

- ***Localization:-***

By their physical location smart things are familiar, and it could be pinpointed. The mobile phone network or the GPS as well as ultrasound time estimations, UWB (Ultra-Wide Band) and optical techniques are suitable to achieve this.

- ***User interfaces:-***

With mankind a set of smart objects can be connected in a suitable aspect which can be either directly or in- directly through a smart phone. Here flexible polymer- based displays, image recognition methods, tangible user interfaces like variational interaction patterns are relevant.

The implementation of all of the abilities are often excessive and requires significant technical power thus in most of the precise applications only needed a subset of these abilities. Applications which having a logistic approach are can be currently engrossed in the approximate localization and using RFID or bar codes relatively low-cost identification of objects is possible. Sensor data are bounded to those logistics applications where such information is important. (Miorandi; Daniele; Sabrina Sicari; Francesco De Pellegrini and Imrich Chlamtac.,2012).

B. Security Challenges in IoT:-

For enabling the IoT technologies appropriation to a great extent, security services serves as a captious component (Miorandi; Daniele; Sabrina Sicari; Francesco De Pellegrini and Imrich Chlamtac.,2012). If there is no assurance in the terms of system-level then the confidentiality of information, authenticity of information and its privacy, and the pertinent stakeholders have to embrace solutions for IoT unlikely on large degrees.

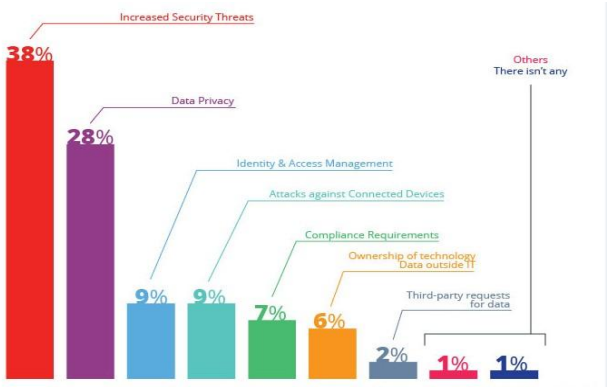


Fig 3: Internet of Things - Top Security Issues

In the early-stage of deployments in IoT the example, is based on RFID technologies only, thus the solutions are mostly seen in an adhoc manner. This shows that such deployments were vertically assimilated, with all constituents under the management of a single administrative entity. Thus a revealed IoT eco- system, where the diverse actors may be involved in a given application scenario then a number of security demands do arise. (Sicari.S ; Rizzardia.A ; L.A. Grieco and A.Coen – Porisini., 2015) Figure3. shows the top governance security issues with the Internet of Things architecture. Among objects and users IoT capacitate sharing of data in order to acquire particular objectives. And in such an atmosphere for the secure communication the security properties such as authentication, the technique of access control, authorization and process of non- repudiation are important (Sicari.S ; Rizzardia.A ; L.A. Grieco and A.Coen – Porisini., 2015).

Thus the major security challenges in IoT include:

a) ***Data Confidentiality****:* The security goal that rep- resents confidentiality of data is an important issue in Iota scenarios, which indicate the certainty that only authorized entities can have the access and make modification to data. In the IoT context not only the person who uses Internet- services, and also the authorized objects may access the data. And this requires the addressing of two important aspects such as the description of a mechanism for controlling access and the explanation of an object authentication process. To the physical realm, the data stored or used in IoT scenarios will be connected for ensuring confidentiality of data and this is a primary constraint for many applications.

b) ***Authentication****:* The various multiple entities involved in an interconnected framework, such as data sources, information processing systems, service providers and when they need to authenticate each other, it is essential to know that how identity to be verified and authentication management can be done in the IoT, in order to assure the services exchanged each other. When these all security mechanisms are defined, we also have to consider some of the immanent features of the IoT. As the interactions are vigorous, and thus in

advance the entities of the network doesn't know who ever can be used for creating a service. (Miorandi; Daniele; Sabrina Sicari; Francesco De Pellegrini and Imrich Chlamtac.,2012)

c) ***Access control:*** The term access control assigned to different peer entities deals with the usage count of resources based on permissions. There are mainly two subjects identified in this. One of them the data holders and the other is the data collectors. The things must be able to feed only with the data behold a specific objective to the data collectors. And simultaneously, the collectors of data must be able to authenticate users and things as legitimate ones. In IoT we also have to deal with the streaming data processing but in traditional database systems it deal with with discrete type of data. In this context the main critical issue that refer to evaluate the performance and temporal constraint is the control of access for a data stream and this is more computational comprehensive than this traditional Database System.

d) ***Privacy:*** The term privacy of data mainly defines the various guidelines through which the access of data referring to individual users happens. The major reason that makes this security property a fundamental IoT requirement mainly based on used technologies and envisioned IoT application areas. The applications on Health-care represent the most outstanding field of application, where the adequate mechanisms are lacked for ensuring the privacy of sensitive information has harnessed the IoT technologies acceptance. In addition, wireless communication technologies have a prominent role. In term of privacy violation the ubiquitous adoption of the wireless medium for exchanging data may pose new issue. Also, as the wireless channel increases due to the remote access capabilities the risk of violation also increases, that expose the system to masking attacks and eavesdropping. Thus privacy indicates an open issue that limits the IoT development.

e) ***Policy Enforcement:*** For a set of defined actions the policy enforcement deals with mechanisms that are used to force it. And the policies are needed to be enforced for maintaining the order purpose, security, and stability on data. Security services such as authentication of data, encryption on data, antivirus software and firewalls is proposed to use for protecting the confidentiality, availability and integrity of data.

f) ***Trust:*** With use of different meanings the concept of trust can be used in a large number of different scenarios. Even if its importance has been widely recognized it shows complex consideration towards the information science literature and computer. On the adopted vision diverse explanations are possible. Towards trust definition many problems exist. One of the major problems is that they do not accommodate themselves to the evaluation methodologies and establishment of metrics. This refers to the security policies govern accesses to resources and credentials. And negotiation on trust make mention of to the process of interchanges of credentials for acquiring service to provide the necessary credentials for a party requiring a service from another party.

g) ***Secure middlewares in IoT:*** There normally within the IoT framework uses large number of diversified technologies, several types of middleware layer that are employed to constrain the data integration and the security of devices and data related. The data must be exchanged within such middle- wares with strict protection constraints. And also in the design of middleware and its development, the diverse communication mediums need to be considered. (Sicari.S ; Rizzardia.A ; L.A. Grieco and A.Coen – Porisini., 2015)

h) ***Mobile Security in IoT****:* Mobile nodes sometimes move from one cluster to other, to provide identification, authentication, and privacy protection in which cryptography based protocols are required.

B. IoT Attacker Models:-

It is very much important to analyze and recapitulate the attacker models in IoT framework. These attacker models have been explained in a way that they can be applied to both coordinated as well as distributed scenarios.(Roman; Rodrigo; Jianying Zhou and Javier Lopez., 2013) Because of an attacker can administer only the part of the network, thus it is inconceivable for an attacker to control the whole system altogether. Thus an attacker can be both from internal and also from external network at the same time. Thus these attacker miniatures, grouped by threats, can be described as follows:

- ***Man-in-the middle attack (MITM):***

The keying material as well as security and domain specifications could be eavesdropped when the various devices are appointed into a network. The secret key between the devices can be disclosed by this keying material and the authoritativeness of the communication channel sometimes could be compromised. And one

type of eavesdropping is possible through this man-in-the-middle attack in the appointment of new devices to the IoT. In this attack the key establishment protocol is vulnerable. All the devices usually do not have prior knowledge about each variants and this can compromise device authentication. As authentication of device involves reciprocating of device individualities, due to man-in-the-middle attack identity theft is also possible.

- ***Denial of Service(DoS):***

Against the IoT there are a distended number of service denial attacks can be launched. Apart from traditional Internet service denial attacks that enervate network bandwidth as well as service provider resources, the absolute wireless infrastructure of most data acquisition networks can also be targeted. One of such an example scenario is jamming the channels. And the low memory and limited computation resources having objects in IoT, they are vulnerable to resource enervation attack. So as to consume their resources the attackers can send to specific devices various messages. This DOS attack is demoralizing in Iot because sometimes attacker capacity may be single and they are large in numbers in resource constrained devices. Due to man-in the-middle attack DoS attack is also credible. The internal attackers who are malicious that take control of part of the infrastructure can concoct even more confusion.

- ***Replay Attack :***

The identity cognate information or other credentials when exchanged in IoT, this can be spoofed or re- played to confront network traffic. This may result in a very serious replay attack. It is also a form of man- in-the-middle attack. And these replay attacks can be prevented by maintaining the newness of random number, by using time stamp or nonce by including message Authentication Code (MAC).

- ***Physical damage:***

This threat is considered as a subpart of the service denial attacks. In this model, effectual attackers block the provisioning of IoT services by destroying the actual things usually by deprive technical knowledge. This is a hard-headed attack in the framework, because things could be effortlessly accessible to anyone. And also the attacker can create a virtual device for targeting the module. (Roman; Rodrigo; Jianying Zhou and Javier Lopez., 2013).

- ***Eavesdropping:***

In order to extract data from the information flow the attackers can target various communication channels such as wireless networks, local wired networks, Internet. And this attack is passive because they don't modify the data. Thus obviously, an internal attacker will be able to extract the information that circulates within it.(Roman; Rodrigo; Jianying Zhou and Javier Lopez., 2013).

- ***Node Capture:***

The things that mainly include household appliances, street lights which are physically located in a certain environment. An active attacker can try to take out the data they contain without destroying it. Infrastructures that store information are also targeted by active attackers, such as data storage entities.

- ***Controlling:***

If there is a path of attack, functioning attackers can gain over an IoT entity the partial or full conduct. The latitude of damage caused by these attackers relies upon the consequence of what all data managed and the services provided by that particular entity.

Authentication properties and objective of authentication in IOT:-

A. Authentication Properties:-

The expression of the future is digital; and with emerging technologies, this will comprehend interconnected devices that automate the administration of the appliances and devices we depend on every day. The dawn of an era where the items are communicating among themselves with little human interaction can be seen. Emerging technologies are spinning the Internet of Things (IoT), to the Internet of Everything. The IoT bear to life a vision of the future where the more physical aspects of life can be automated so we can enjoy more meaningful existing. Through widespread progress in smart technologies, the generation to a fully connected world is advancing in hurry. As the IoT become more common place in the devices we use habitually, it will increase the number of targets for data security combination. During the interconnections, the Iot is suffering from severe security challenges, there are potential vulnerabilities due to the entangled net- works make reference to diverse targets, sensors and backend management systems. Network security and also the use of surviving connectivity security protocols are essential to

secure IoT. The credentials that are interchanged between the various devices can be made secure by establishing these security extents. These measures include authentication, authorization and encryption. Authentication means assuring the individuality of users, machines or applications try to access the exchanged information. Authorization means assuring that the users, devices and applications have allowance to access the exchanged information. Encryption means assuring that information is only comprehensible by authorized parties and cannot be intercepted.

B. Objective of Authentication in IoT:-

In association with these three security measures authentication has an important part. Authentication is the operation to verify the digital uniqueness of an entity. Here the term entity represents the things interconnected in IoT context. Thus by using proper authentication structure it can be guarantee that whether someone or something is, in performance, who or what it is declared to be. And the outcome of an authentication protocol will be acceptance or rejection. The authentication protocol developed for the IoT framework should provide bottom-up security in all means. Thus the information that is exchanged between the various interconnected devices can be secured from security attacks such as snooping, traffic analysis, modification, replaying attack etc. Another challenge in IoT security is to acknowledge consumers to use the security integrated into their devices.

C. Types of Secure Authentication Schemes for IoT environments:-

A. Novel Mutual Authentication Schem:-

This provides a novel mutual identity authentication scheme which can be applied in IoT steadily and securely. Secure hash algorithm, Cryptography based on Elliptic curve and extraction of features are the basic principles used by this scheme and thereby proposing mutual authentication scheme which is asymmetric between the terminal as well as platform entities, which establishes light computation and communication cost. Platform identity authentication and terminal node identity authentication is involved in this scheme. Here the attacker may insert end nodes that are invalid into the sensor network to delude platform and other entities so the end entities also should be authenticated mutually. (Guanglei Zhao.,2011). By processing message block of 512 bits here uses SHA-1 algorithm which produces a 160 bit hash function (message digest).It is infeasible to find a message corresponds to a message digest by using SHA-1 and it is also infeasible to find two different messages with same message digest. And the extraction of features is a technique used in image processing and pattern recognition. Using this technique the set of features can be derived from input data in order to accomplish desired work using this reduced representation instead of full size input. In this mutual authentication scheme the exert of this feature extraction are mainly based on two aspects: firstly, by , extraction of feature the original quantity of information can be diminished, by which information forwarded over the wireless network will be less; secondly, the original message sent cannot be recaptured after feature extraction because it is an irreversible process. Therefore, if to other nodes we send this information, the feature of the information which is estimated from the hash functions cannot be obtained by the attacker even after it interrupts the transmitted information. The proposed mutual authentication scheme is shown in Figure 4. For hash functions this scheme can defend against collision attack and with some method for feature extraction, the increased consumed resource can also be limited. This scheme can't use the public key system based authentication scheme, because much resource is needed for public and private key computation, which is not appropriate for end nodes in IoT. (Guanglei Zhao., 2011).

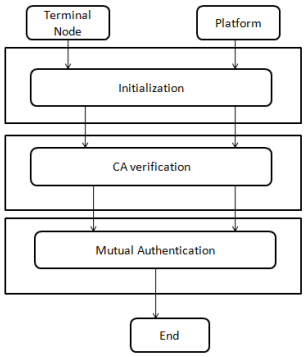


Fig 4: Mutual Authentication Scheme for IoT

The advantages of this scheme include security for applications, computation steps are limited and hence less memory resource is consumed. The Irreversibility of SHA-1 and feature extraction, helps avoiding if an attacker pretend to be an end node and perform impersonation attack. And because it is computationally infeasible to find two entities that compute same hash value and thus collision attack avoidance can be done for hash functions. And also because of the random factor in authentication information prevent replay attack. The main disadvantage is that it is not suitable for the terminal entities in IoT, because the authentication scheme cannot use public key cryptosystem.

B. Directed Path Based Authentication Scheme:-

Based on layered U2IoT architecture (i.e., Unit IoT and Ubiquitous IoT) this scheme is considered, and to realize security protection proposed a directed path based authentication scheme (DPAS) for the U2IoT architecture. An U2IoT architecture which is human-society inspired is proposed (as shown in Figure 5).In the U2IoT architecture, to establish the single as well as multiple application scenarios mankind neural system and social organization framework are introduced. A local IoT within a region for an industry is formed by multiple IoTs. To form the ubiquitous IoT the local and industrial IoTs are covered within the national IoT in the architecture, for a single application the unit IoT refers to a network unit base, and the ubiquitous IoT deals within the centralized national management many applications. Here particularly, for the secret key distribution and cross-network authentication the directed path descriptor is introduced, and the proof mapping is applied to establish tri-dimensional equivalence relations among diverse nodes for mutual authentication. This DPAS scheme is shown in Figure6 which provides data confidentiality and integrity, authentication, anonymity and forward security. And the performance analysis of DPAS indicates that with moderate IoT applications communication overhead and computation load is suitable. (Huansheng Ning; Hong Liu.,2012).

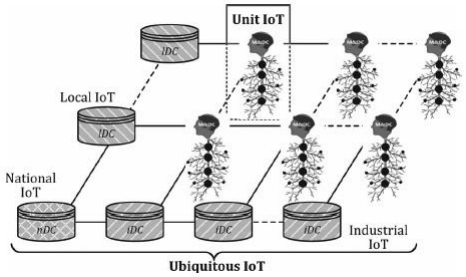


Fig. 5. The U2IoT architecture
(Huansheng Ning; Hong Liu; Yang L.T.,2015)

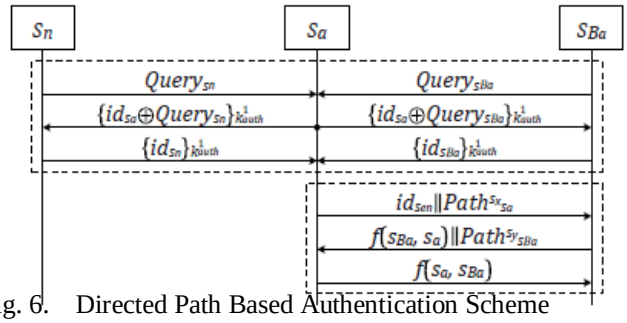


Fig. 6. Directed Path Based Authentication Scheme

The above discussed scheme provides data confidentiality by the use of strong master key and data integrity by using hash functions, because of that the legal nodes will not deduce the inconsistent values and also recognize the illegal attacker even if robust attacker succeeds to modify the exchanged data. But it doesn't provide mutual authentication between the sensor and terminal nodes.

C. Aggregated-Proof Based Hierarchical Authentication Scheme for the IoT

For layered IoT architectures this provides a hierarchical authentication scheme. An existing U2IoT architecture is also focused here. Homomorphism function and Chebyshev polynomials form the base of this scheme. The relationships of directed path descriptors, group identifiers and pseudonyms are represented using these parameters.

By the use of Chebyshev chaotic maps and directed path descriptors wrapped by the homomorphism function this authentication scheme provides data confidentiality and data integrity. For enhancing session randomization the pseudo random numbers generated. And by one-way hash function data integrity is achieved. By two layer interactions this scheme provides hierarchical access control and each entity have its own access authorities. Forward unlink ability is also provided by this scheme using pseudo random numbers to provide session freshness and randomization which are generated as session-sensitive operators .Thus the ongoing sessions with former sessions cannot be correlated by an attacker in the open channels. Between the sensors and the targets this scheme also provides mutual authentication. By using backward and forward aggregated proofs also provides privacy preservation. Thus identity related information is kept secret among layered entities. Two sub- protocols are designed for unit IoT and the ubiquitous IoT in this Hierarchical authentication scheme based on Aggregated- Proofs (APHA) (Huansheng Ning; Hong Liu; Yang L.T., 2015). This scheme provides bottom-up security protection for the entire IoT framework.

This scheme is best suitable for layered architectures. Also data confidentiality, integrity, mutual authentication, forward security and privacy preservation like security properties are provided.

D. Identity Authentication and Capability Based Access Control (IACAC) for the IoT

In the context of IoT authentication of data and control in access are important and critical functionalities to enable the communication between devices more secure. The possible sources for security vulnerabilities in IoT networks are the mobility, the topology of dynamic network and of low power devices' weak physical security. This scheme provides authentication of data and in a resource constrained and distributed IoT environment it is light weight as well as access control attack resistant. This scheme is the Identity Authentication and Capability based Access Control (IACAC) model toprotect IoT from impersonation attack, replay and denial of service (Dos) attacks, here also introduced the concept of capability for access control. It presents an integrated approach of authentication and control in access rights for IoT devices; this is the novelty of this model. Elliptic curve cryptography- Diffie Hellman Algorithm (EC- CDH) is used to generate the secret key in this scheme. This ECCDH is a symmetric key agreement protocol to generate a secret key that is kept shared and which can be used by each other by two devices that have no knowledge about each other in prior. The secret that is shared can be calculated using this public parameter and owned private parameter. Any third party cannot calculate the secret that is shared from available public information who doesn't having access to each device's private details. Mutual authentication is also provided by this scheme between the devices.Thus device authentication along with credential transfer is provided by this scheme. (Parikshit N. Mahalle ; Bayu Anggorojati ; Neeli R.Prasad; Ramjee Prasad., 2013) .

For the above discussed scheme, with relation to their location and time when new devices join to IoT framework, security bootstrapping is applicable. And also between devices one-way and mutual authentication is provided. And from the man-in-the middle attack, replay attack and DOS attack protection is provided. But from passive attacks protection is not provided.

E. Improved Identity Authentication scheme for IoT in Heterogeneous Networking Environments

Rather than RSA, Elliptic curve cryptography technique is used in this improved technique of identity authentication scheme. This scheme is effective and safe for heterogeneous environments. This scheme works on both public and private key pair. This identity scheme has its own public key which is known and a private key which is not open. It provides data confidentiality, data integrity, data timeliness, network robustness. (Fuzhi Chu; Runtong Zhang; Rongqian Ni ., 2013)

This scheme provides security against passive attacks. The strength of Elliptic Curve Cryptography Discrete Logarithmic Problem (ECDLP) is used for providing security, and thus if the attacker intercepts the authentication information to get private key of nodes involved it is infeasible. By providing security against replay attacks, it is impossible to crack user's private key. But against active attacks security is not provided.

F. Device authentication scheme for smart IoT network

This scheme provides a robust and secure authentication scheme for smart energy home area networks (SE-HAN). Here uses ECC and self-certified public key technique for authentication and key establishment. The proposed scheme can be divided into different stages including prior to deployment stage, the initialization phase, authenticated key reconciliation, key renewal and revocation mechanisms which are controlled by the user. In the pre-deployment stage, in order to acquire an absolute certificate for every smart device it has to contact the certificate authority. During the smart home device deployment the initialization stage enters. In this phase the long term public/private keys and useful definite certificates are computed by the device. It generates an authenticated key (AK) which is two-pass between the smart devices during the authenticated key agreement phase. And then the

key renewal and key revocation mechanisms can be performed if needed. Authors claimed that when compared with other authentication schemes (Binod Vaidya; Dimitrios Makrakis; and Hussein Mouftah., 2012), (M.A. Strangio) their scheme is efficient. When evaluated the proposed scheme based on computation efficiency, it shows that the Elliptic Cryptography scheme increases the processing time of each edge thing when authenticated. And also this scheme doesn't provide much details regarding how it is efficient than others (S. Wang et al., 2008) and how is it secure against attacks.

Item	AK scheme for	MQV	ECK	ECKEI
KKS	Yes	Yes	Yes	Yes
UKS-R	Yes	No	Yes	Yes
FS	Yes	Yes	Yes	Yes
KCI-R	Yes	Partial	No	No

Table I. Comparison of security properties of AK scheme in SE-HAN system.

The above table 1 shows the comparison of security properties of the proposed scheme when compared with other key agreement protocols such as MQV(A ZigBee based scheme) (Binod Vaidya; Dimitrios Makrakis; and Hussein Mouftah., 2012), Efficient Diffie-Hellmann key agreement two- party protocol (ECKEI) (M.A. Strangio) based on Elliptic curves and another improved ECKEIN (S. Wang et al., 2008) scheme based on elliptic curves. The security attributes considered are known-key security(KKS), key-compromise impersonation resilience (KCI-R), unknown key-share resilience (UKS-R), forward security (FS) etc.

G. Key establishment protocol for smart IoT system:-

This scheme proposes a key establishment protocol for smart home energy management systems. When considered the security of smart home energy management systems the major issue is the initial session key establishment between things and the server. Most of the protocols that focus on security in computer system and internet safeness cannot be implemented in smart home applications because they are very much expensive. On Zigbee-based local home networks, the conventionally used PKC (Public Key Cryptography) key establishment protocols cannot be implemented directly. The proposed scheme consists of two phases. In the first phase, each device securely contacts with Certificate Agent (CA) and obtains public or private key pair. And then the device and controller unit carry out a key exchange protocol. In the second phase authenticates themselves for establishing an initial session key. There also shows a comparison among the Eldefrawy etal.'s, Hang and Huang Key-establishment schemes with this proposed SHEM scheme which is described in the below given Table 2.

Item	KE	Eldefrawy	Hang et al.'s	Huang et al.'s
Group Key Agreement	Yes	No	No	No
Mutual Authentication	Yes	Yes	Yes	Yes
Avoiding replication attack	Yes	Yes	No	No
Avoiding masquerade attack	Yes	Yes	Yes	Yes
Forward Secrecy	Yes	No	Yes	Yes

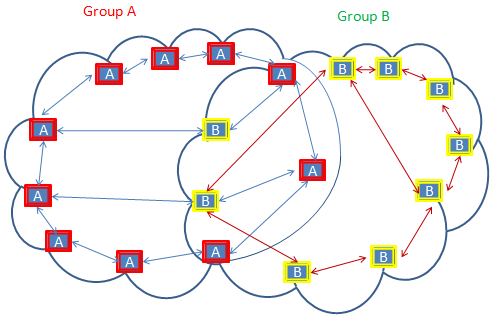
Table II. Comparison of security properties of KE scheme in SHEM system

H. Threshold Cryptography-Based Group Authentication (TCGA) Scheme for the IoT:-

In the IoT due to unbounded number of devices; each device cannot be authenticated in the short time. And at the same time, it is also hard to get reply for authentication request. Thus this TCGA scheme provides a safe and efficient authentication strategy that verifies at once the authenticity of a group of de- vices in a context of IoT where resources are constrained. This TCGA scheme is provided for Wi-Fi environment. Here uses Paillier Threshold Cryptography the (t,n) threshold scheme where t represents the threshold and n is the group of members which is a public key variant. This is an asymmetric public key encryption scheme that uses impermanence in an encryption algorithm, when encrypting thus different cipher texts will be retrieved for same plain text for many times. This cryptosystem assists to achieve homomorphic holdings, thus provides privacy preservation. The TCGA comprises five different modules; Key Distribution, Key Update, Group Credits generation, Authentication Listener and Message Decryptor phases.

When any precise individual in a group, wants to initiate a group activity, a request is send to the Group Authority(GA) which one is present. When the request is received, the GA creates a secret for session that is to be shared by all the individuals of the group. Using the public key of the group, then encrypt the session secret for providing the needed security as only by using the complete private key it can be decrypted. Then a hash function is applied to the secret to prove the integrity of this message which is going to be used in further steps. Then in a single message, it is sent with the encrypted session. Then it is sent to all the individuals of the group.

Then all the devices decrypt this session secret which gives them a partly decrypted message (PDM) using their own part private keys and which will not be the session secret that is final. Then this PDM is send to each member in the group, each of the devices in the group waits until n-1 PDMs are received. In the group all the devices then try to collect all of the shares through the final session secret which should be known ultimately. If successful, means that the received PDMs are by the legitimate group members only, the group authentication succeeds. Then the group activity can then be started for further communication using the session secret. Figure 7. shows the group authentication. If not successful, means there be one device at least which uses part private key which is fake and thus the partial decryption also generated by him is not genuine. Thus when try to combine all the shares it was a



failure. Then the group authentication fails, and there requires restart of the process. (Parikshit N. Mahalle; Neeli Rashmi Prasad ;Ramjee Prasad., 2013)

Fig. 7. Group Authentication

It removes the need to establish secure connection b/w all devices in a particular group whenever they want to communicate. Thus conserve power by reducing overhead by ensuring minimum no: of resources are used. Here dynamically changes the session key when each new group activity is initiated thus providing security from replay attack. Also provides security from the impersonation attack.

Discussions:-

The section provides a brief comparison between the various authentication schemes discussed so far. Table 3 shows a comparison among the discussed authentication schemes in literature. The Cryptographic algorithms (both symmetric and asymmetric) play an important role in providing authentication services. The main problem with this is the conventional public key assignment. The cryptographic systems used in authentication schemes is that in order to have high security the key size has to be sufficiently large. Thus consumption of more bandwidth and less speed occurs. Then used Elliptic Curve Cryptography Technique as a solution for this. And the various authentication schemes that are constructed based on the hardness of the following mathematical problems. The RSA algorithm depends on the intractability of integer factorization problem. The DH protocol relies on the hardness of discrete logarithm. Due to the elliptic curve discrete logarithm problem (ECDLP) the ECC is secure. The direct way to break the scheme is to draw the private key from the public key present. But the computation cost required is same as solving these difficult mathematical problems. Thus ensures security from different types of attack in IoT environment .

Scheme	Algorithms	Security from attacks
Mutual [5]	SHA,Feature Extraction	MIM, Replay Attack
DPAS [6]	Symmetric Key generation	Replay attack
APHA [7]	Symmetric Key generation	Replay attack, MIM
IACAC [8]	Diffie-Hellman exchange	DoS, Replay, MIM
AK [19]	ECC,Public key	MIM

KE [20]	Asymmetric	Replay attack, Masquerade
TCGA [10]	Asymmetric	MIM, Replay attack

Table III. Comparison on Authentication Schemes for IoT

Conclusion:-

In an Internet of Things background a variety of devices and appliances are interconnected and these things can assemble data, communicate and build decisions with or without human interactions. Based on the application necessities in various IoT scenarios different authentication schemes are needed. And these authentication schemes should supply security against the various IoT attacker models. Here by considering the security challenges in Internet of Things and discussing the various attack scenarios and also the comparison study of different authentication schemes.

Acknowledgment:-

We would like to thank God for all the help rendered in choosing and grasping information. We would like to thank our college for helping us with all the resources and our family members who have been very patient during this work.

References:-

1. **Miorandi; Daniele; Sabrina Sicari; Francesco De Pellegrini and ImrichChlamtac.(2012)** "Internet of Things: Vision, applications and research challenges"; published on Ad Hoc Networks 10, On page(s):1497-1516
2. **Atzori L; Antonio Iera; Giacomo Morabito. (2010)** "The Internet of Things:A survey"; published on Journal of Computer Networks 54 ,On page(s):2787-2805.
3. **Zheng; Yan ; Peng Zhang and Athanasios V.Vasilakos . (2014)**, "A survey on trust management for Internet of Things";published on Journal of Network and Computer Applications 42. On page(s):120-134.
4. **Sicari.S ; Rizzardia.A ; L.A. Grieco and A.Coen-Porisini . (2015)**, "Security, privacy and trust in Internet of Things: The road ahead";published on Computer Networks 76 , On page(s):146-164.
5. **Guanglei Zhao .(2011)** " A Novel Mutual Authentication Scheme for Internet of Things" ; Proceedings of 2011 International Conference on Modelling, Identification and Control,06
6. **Huansheng Ning;Hong Liu . (2012)** "Directed Path Based Authentication Scheme for the Internet of Things";Journal of Universal Computer Science,vol.18,no.9, On page(s):1112-1131.
7. **Huansheng Ning; Hong Liu; Yang L.T.(2015)** "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things", Parallel and Distributed Systems, IEEE Transactions on, On page(s): 657 - 667 Volume: 26, Issue: 3, March.
8. **Parikshit N.Mahalle ; Bayu Anggorojati ; Neeli R.Prasad; Ramjee Prasad. (2013)** "Identity Authentication and Capability Based Access Control(IACAC) for the Internet of Things"; published on Journal of Cyber Security and Mobility,vol.1, On page(s):309-348.
9. **Fuzhi Chu; Runtong Zhang; Rongqian Ni; Wei Dai .((2013).** "An Improved Identity Authentication Scheme for Internet of Things in Heterogeneous Networking Enviornments" , 16th International Conference on Network- Based Information Systems.
10. **Parikshit N. Mahalle; Neeli Rashmi Prasad ;Ramjee Prasad. (2013)** "Threshold Cryptography based Group Authentication(TCGA) Scheme for the Internet of Things".
11. **Kiho Lee1; Ronnie D. Caytiles1; Sunguk Lee. (2013)**"A Study of the Architectural Design of Smart Homes based on Hierarchical Wireless Multimedia Management Systems"; International Journal of Control and Automation Vol.6, No.6, pp.261-266.
12. **Sukhvir Notray ; Muhammad Siddiqiy ; Hassan Habibi Gharakheiliy ; Vijay Sivaramany; Roksana Boreli . (2014).** "An Experimental Study of Security and Privacy Risks with Emerging Household Appliances" Workshop on security and privacy in Machine-to-machine communications.
13. **Hyungkyu Lee; Jooyoung Lee; Jongwook Han.(ICNC 2012)** "The Efficient Security Architecture for Authentication and Authorization in the Home Network" Third International Conference on Natural Computation.
14. **Friedemann Mattern. (2010)** "From the Internet of Computers to the Internet of Things",Lecture Notes in Computer Science.
15. **Young-Pil Kim; Seehwan Yoo ; Chuck Yoo .(2015)**"DAoT: Dynamic and Energy-aware Authentication for Smart Home Appliances in Internet of Things" IEEE International Conference on Consumer Electronics (ICCE).

16. **Kemal Altinkemer ;Tawei Wang . (2011).** "Cost and benefit analysis of authentication systems";published on Decision Support Systems 51,On page(s): 394-404.
17. **Roman; Rodrigo; Jianying Zhou and Javier Lopez. (2013)** "On the features and challenges of security and privacy in distributed Internet of Things",published on Computer Networks.
18. **Binod Vaidya; Dimitrios Makrakis; and Hussein Mouftah . (2012)** "Secure remote access to Smart Energy Home area Networks"; Innovative Smart Grid Technologies (ISGT), IEEE PES. IEEE.
19. **Vaidya; D. Makrakis; and H.T. Mouftah. (2011)** "Device authentication mechanism for Smart Energy Home Area Networks"; In Proc. IEEE International Conference on Consumer Electronics (ICCE 2011), pp. 787- 788.
20. **M.A. Strangio**. "Efficient Diffie-Hellmann two-party key agreement protocols based on elliptic curves"; In Proc. ACM Symposium on Applied Com.
21. **S. Wang et al. (2008)** "Cryptanalysis and Improvement of an Elliptic Curve Diffie-Hellman Key Agreement Protocol"; IEEE Communication Letters, 12(2), pp. 149-151.
22. **Y. Li . (2005)** "Design of a key establishment protocol for smart home energy management system"; Proc. 5th Int. Conf. Comput. Intell; Commun. Syst. Netw. (CICSyN) ; pp.88 -93 puting; pp. 324-331.
23. **M. Wang; G. Zhang; C. Zhang; J. Zhang; C. Li (2013)** "An IoT-based Appliance Control System for Smart Homes" ; ICICIP.
24. **K. Han; J. Kim; T. Shon and D. Ko. (2013)** "A novel secure key paring protocol for RF4CE ubiquitous smart home systems"; Pers. Ubiquitous Comput; vol. 17 ; no. 5 ; pp.945 -949.
25. **Rafiullah Khan; Sarmad Ullah Khan; Rifaqat Zaheer; Shahid Khan. (2012).** Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges , 10th International Conference on Frontiers of Information Technology.
26. **Meng Chu Zhou. (2013)** Internet of Things: Recent Advances and Applications Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design.