Secure and Scalable Authentication for Data Privacy in IoT-Driven Wireless Sensor Networks

John Smith[1], Maria Garcia[2] and David Johnson[3]
[1]Department of Computer Science, University of Oxford, United Kingdom
[2]Department of Electrical Engineering, Universidad de Buenos Aires, Argentina
[3]Department of Information Technology, University of California, USA

ABSTRACT

The security of IOT raises the major concerns as the IOTs are equipped with the limited resources based sensor nodes. Hence, these sensors must be provided with the light and efficient security algorithm for the enforcement of data privacy and user integrity in the given network. The two major security paradigms for IOTs are authentication & encryption mechanisms, which have many variants. In this thesis, the work has been carried over the enhancement of the proposed security model by designing the authentication model with set of algebraic equations. The multi-column based complex key generation is designed around the algebraic equations, specifically cubic and quartic equations. The authentication keys and data encryption is another security paradigm of the proposed model, which utilizes the advanced encryption standard (AES), which has been used for the implementation of the high security protocols. The performance of the proposed model has been analyzed under the different scenarios with variable number of nodes (50, 100 and 150) with decreasing transmission range of 75, 50 and 25 respectively. The proposed model has been recorded with minimum projected resource readings at 1.09, 5.49 and 10.96 percent in the scenarios with 50, 100 and 150 nodes respectively, whereas the maximum readings are 1.95, 9.81 and 19.63 percent for similar scenarios.

Keywords: Authentication, Peer to peer security, Complex key, Mutual Authentication.

I. INTRODUCTION

The 20th century saw the change of the hospital system due to the primary healthcare monitoring within the United States. The centralization of medicine into massive facilities reflected the changes in structure of society from primarily rural to primarily urban. (Lee et al. 2014). In the 21st century, there is increase in different healthcare systems which is supported by different infrastructures. The distribution of healthcare is turning into great facilities, which is reflecting the change in structure of society. The sociology of the population is dynamic , from a younger population to elderly ones.(Abomhara , Mohamed and Geir M. Koien 2014).

Many recent articles have described the dilemma of illness and the care of different diseases,(Khan et al. 2014) that notices rising costs and gaps within the healthcare system. The problems are not only those of cost, but also of coverage, access, tracking, security and information. Tracking health status can be supported by “Health Monitors”, that is periodic checkup is being performed concerning each patient’s health, where the patient must remember its symptoms as the doctor performs some check and formulates a diagnostic, then monitors patient progress along the treatment. Above system is technically performed by some embedded technologies, including: (Hemandez et al. 2015).

- Sensors that collect patient data
- Microcontrollers process, analyze the data
- Wirelessly communicate the data
- Healthcare-specific gateways through which sensor data is further analyzed and sent to the cloud

The security of Internet of Things (IOT) can be traded off from various perspectives by (Kim et al, 2012)A remote end client getting to base station data can be kept from doing as such in an assortment of ways. Correspondence between the base station and IoT sensor nodes can be blocked. This can be proficient by simple sticking of signs or by computerized sticking as DoS (Denial of Service) assaults that surge the system, base stations or both. Directed DoS assaults on key hubs in the IOT can likewise piece correspondence of huge parts of the system with the base station. Correspondence between base stations and other IoT sensor nodes can be averted by setting up erroneous directing data with the goal that movement goes to the wrong goal or circles. One approach to do this is to parody the base station and beguile hubs into rerouting all bundles to the caricature base station rather than the genuine base station described by (Manikandan et al., 2014).

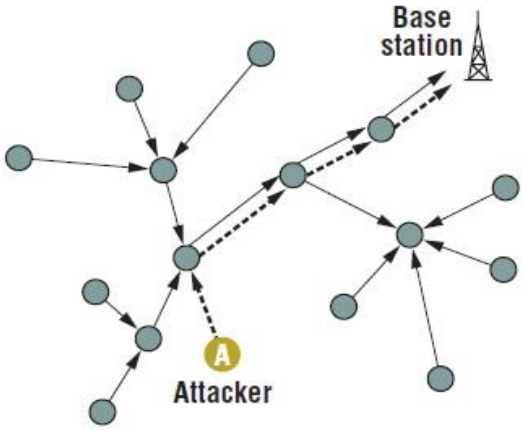

Figure 1:Attacks on Internet of Things

Another method for breaking security is to decimate the base station itself. This can be proficient by checking the volume and bearing of parcel activity toward the base station so that the area is in the long run uncovered by (Benitez, 2001) Destruction can likewise be proficient by tuning in to the RF signs to limit and triangulate the area of the base station. A third risk is listening in. This is made less demanding by remote bounce to-jump correspondence. Listening stealthily can be utilized to track and derive the area of the base station for demolition. There are numerous different strategies to rupture the IOT security is characterized by (Yi,Jae, and Saniie, 2013).

Assault on IOT can be happening in various techniques. IOT is inclined to security assaults which are submissive in character by (Benitez, 2001).The most natural security assaults on IoT sensor nodes is Monitor and Eavesdropping in this assault the adversary could without much of a stretch discover the data content by snooping the data. Security of IOT is the most noticeable issue. The Security assaults which occur on remote system are of unmistakable sorts. False steering Information is a Routing Attacks in Sensor Networks the programmer change the directing information of steering conventions through malignant code. Wireless system is likewise undermined by Sybil Attacks through this assault a delicacy of single hub is made and speaks to its various personalities to different hubs in remote system by (Kumar et al., 2012) . Wormhole assault the foe hold data from one area in the system transmit into another area and on the other hand retransmit into the system. Specific Forwarding is a dynamic assault in this sort of assault the programmers assaults the specific hub and contaminate with the vindictive data the irresistible hub act like a typical hub in organize this hub does not forward the parcels or information to next hub it just which make them act like a fizzled hub by (Pandey et al ., 2012).

A Internet of Things (IOT) is an accumulation of IoT sensor nodes, which develops a system utilizing radio correspondence in a self-sufficient and appropriated way. Hubs are appropriated over a particular field, and can gather and hand-off data about the earth, keeping in mind the end goal to give fine-grained perceptions of a wonder. A sensor hub is ordinarily outfitted with at least one sensors that are utilized to catch occasions from the earth, a simple computerized converter, a radio handset, a focal preparing unit with constrained computational abilities, a little measure of memory and a battery control supply. Sensor gadgets work together with each other so as to perform fundamental operations, for example, detecting, correspondence and information preparing.

Real applications utilizing IOTs include: ecological checking, social insurance, state of mind based administrations, situating and creature following, amusement, coordinations, transportation, home and office, mechanical and military applications. Non-meddling and non-troublesome natural checking enables scholars to contemplate touchy untamed life living spaces, for instance the smaller scale atmospheres on Great Duck Island, Maine. Medicinal services applications empower individuals with certain restorative conditions to get steady checking through sensors. Military applications incorporate observation, target following, counter-expert rifleman frameworks and front line checking, in which data is spread to troopers and vehicles required in battle.
The mechanical headways in remote correspondence and microelectronics have brought about a developing enthusiasm for the field of remote sensor systems. A sensor organize includes sending a variety of sensors for circulated checking of constant occasions. The sensor systems have constrained vitality, as the IoT sensor nodes are battery fueled. The IoT sensor nodes likewise have restricted memory and computational ability and can be sent in remote territories or aloof landscape. There has been an expanding utilization of sensor systems forever

basic applications, for example, checking patients in healing facilities and military applications. These applications make it critical to have a decent security framework for sensor systems. The arrangement of these systems in military applications and the restricted power and memory, make the plan of a security convention exceptionally difficult. In this paper security issues in Directed dissemination are tended to. Coordinated Diffusion is a novel directing convention for sensor systems. A look-into conceivable assaults and counter measures is given. The paper is finished up with a concise examination on the conceivable countermeasures to anticipate such assaults.

The security of Internet of Things (IOT) can be traded off from multiple points of view. A remote end client getting to base station data can be kept from doing as such in an assortment of ways. Correspondence between the base station and IoT sensor nodes can be blocked. This can be proficient by simple sticking of signs or by computerized sticking as DoS(Denial of Service) assaults that surge the system, base stations or both. Directed DoS assaults on vital hubs in the IOT can likewise piece correspondence of extensive parts of the system with the base station. Correspondence between base stations and other IoT sensor nodes can be averted by setting up mistaken directing data with the goal that movement goes to the wrong goal or circles. One approach to do this is to parody the base station and betray hubs into rerouting all bundles to the ridiculed base station rather than the genuine base station.

Another method for rupturing security is to annihilate the base station itself. This can be proficient by observing the volume and heading of bundle movement toward the base station so that the area is in the long run uncovered. Devastation can likewise be proficient by tuning in to the RF signs to limit and triangulate the area of the base station. A third risk is listening in. This is made simpler by remote jump to-bounce correspondence. Listening stealthily can be utilized to track and derive the area of the base station for obliteration. There are numerous different strategies to break the IOT security.

Amid the periods when the IOT hubs are in working condition, they require secure cryptographic keys for secure proliferation of the delicate data. Effective key administration and conveyance plot assume a critical part for the information security in IOTs. Existing cryptographic key administration and circulation procedure for the most part devour higher measure of vitality and put bigger computational overheads on Wireless Sensor Nodes. The cryptographic keys are utilized on various correspondence levels of IOT interchanges i.e. neighbor hubs, group heads and base stations. A compelling corporate key administration and appropriation strategy is required to keep up the security of the remote sensor systems.TheIoT sensor nodes likewise have restricted memory and computational ability and can be sent in remote territories or aloof landscape. There has been an expanding utilization of sensor systems forever basic applications, for example, checking patients in healing facilities and military applications.

II. RELATED WORK

Zhou et al. (2013)considerably worked upon the adversary model (AAPM) of the existing work to solve the problem of security when patients traverse among blocks outdoors and perform their regular exercises. A privacy-preserving key management method was developed against time-based and location-based mobile attacks by protecting patient's identity, sensor deployment location etc. It exploited the blinding technique and Blom's symmetric key mechanism for secret sharing. The simulation results proved the efficiency and resistivity against attacks. A mechanism to get rid of patients' selfishness to obtain resistance against mobile compromise attacks was the future requirement of this research.Almashaqbeh et al. (2014)proposed real-time remote health tracking system for non-hospitalized patients. This system divided the cloud architecture as local one that contains patients and hospital medical staff, and a global cloud that contains the outer world. The performance parameters to be optimized were congestion reduction, interference and data delivery delay in mobile sensor network.

Hossain et al. (2014)termed cloud computing through NIST as a model for pervasive, accessible, demand-driven network access to resources such as network bandwidth utilization, storage, software services etc. from shared pool of computing resources that can be easily available with nominal management attempt. The five key characteristics of cloud model were demand-drive services, high bandwidth network access, Resource pooling, Scalability, Measured service.Zhou et al. (2015) introduced a two phase patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) which consists of: an attribute based designated verifier signature(ADVS) scheme that provided three level security in five step algorithm: Setup, Key Extraction, Signature, Verification and Transcript Simulation Generation and the corresponding authorized accessible privacy model (AAPM) adversary model. An access tree was set up defining the access rights supporting threshold attributes for persons based on their belonging category. Directly authorized physicians by patients, indirectly authorized persons and the unauthorized persons can respectively decode with their attribute sets the part of personal health information (PHI) by satisfying the access rights granted to them in access tree.

PSMPA scheme especially proved its success over previous schemes for boosting the energy constrained mobile sensor node's proficiency.

Zarandi et al. (2015)presented K2C (Key To Cloud) -a scalable and lazy revocation based protocol to share and store data securely in untrusted clouds also. Hierarchical Identity-Based Encryption and Key-Policy Attribute-Based Encryption were used for access control, key updation and authorisation. The open source implementation effectiveness was demonstrated over Amazon S3 API. The future research of system was to use proxy re-encryption to improve K2C efficiency and access control protocol by off-loading the task of key distribution to the cloud.Doukas et al. (2015)discussed about the application of Cloud Computing in healthcare services to update and retrieve patient health information. The @HealthCloud application was developed for HTCG1 mobile phone running on Google's Android operating system. Various type of medical images such as MR, OT, CT, PET and Ultrasound were uploaded using WLAN and 3G networks and transmission time taken by both networks was analysed.

Hachem, Sara et. al. (2011) had worked upon the innovative ontological extraction method for IoT networks. In this paper, the authors have worked upon the service oriented middleware application of ontology based IOT network model to describe the flexibility and synchronization ability. The primary focus has been kept upon the ontological modelling of IOTs to describe the variety of features to describe the identity of the nodes along with their network based performance. The multivariate feature descriptor based ontology will be utilized to create the middleware approach. Lim, Léon et. al. (2016) had worked upon the enhancement of internet of things (IoT) with context awareness in the data propagation and distribution network. In this scheme the quality of context (QoC) approach has been utilized to control the context of the data, node or network for the particular traffic flow. This scheme has been designed with the higher order adaptability to handle complex network model consisted of the heterogeneous large-scale IoT environments. Hosseinzadeh, Shohrehet. al. (2016) had worked upon the development of the context-aware mechanism for role-based access control to create the smarter networks, which implements the security framework with semantic ability. In this paper, the data security and privacy model has been developed over the hybrid ontological structure, which includes the device level ontology and web ontology language (OWL). Bernabe, Jorge Bernal et. al. (2016) had worked upon the access control model based upon trust-aware mechanism in the multidimensional approach. This trust aware access control system for IoT (TACIoT) model provides the send-to-end solution with high reliability and security for incorporation of the IoT security model The trust has been taken into account, which is established with the dependability and trust derived on the basis of security oriented considerations, inter-nodal relations, quality of service parameters and IoT node reputation. Xu, Guangquanet. al. (2017) had proposed the semantic model based upon the semantic ontology, which is described over the user defined security rules to ensure the network security among the internet of things with situation awareness.

III. PROPOSED WORK

In this research, we are going to solve the problem of confidentiality and data integrity by mitigating the security threats caused by the shortcomings of the existing diffie-hellman key exchange scheme in the existing IoT based WSN system by adding up various security protocols and algorithms with the existing authentication based on WSN systems.

Methodology

The various steps that are followed are as follows:

Step1: Key exchange to create the session between server and client. This would be done at pre-phase to establish the connection. Keys would be generated into a random fashion. So, it would be non-predictable.

Step2: After step1, the container data would be stored in encrypted format with private key. So, the unauthorized user could not be able to read the data.

Step3: The files would be in read-only format which therecommended process requires to secure the containers content.

Work Flow

The proposed workflow has been demonstrated with the help of flowcharts. First flowchart shown in Figure 2depicts the process of authentication. In this process, key table is generated on both client and server side with random key generator. User tries to create a session after which the server demands key from client and client sends any key from key table.Then, the server matches that key with key table. If key matches,theuser is authenticated. Otherwise, unauthenticated.Second flowchart (Figure 3) presents Detailed procedure of proposed IoT based authentication model.

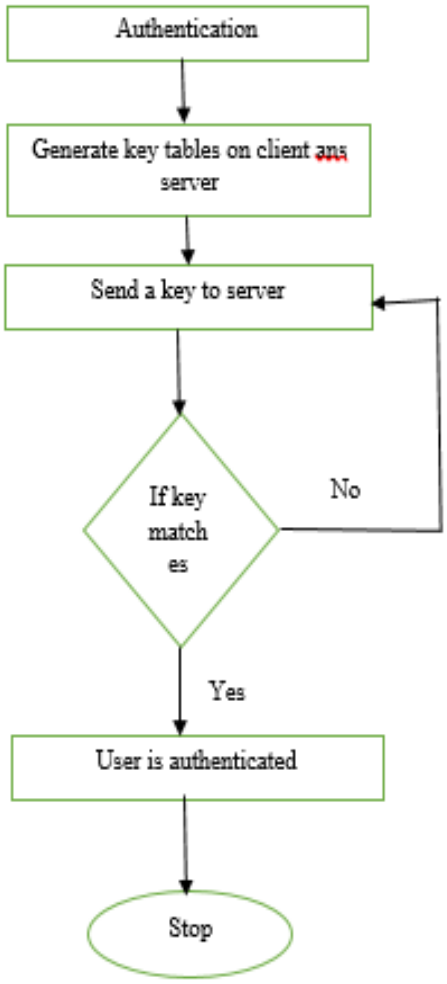

Figure2:Flow chart showing the process of authentication

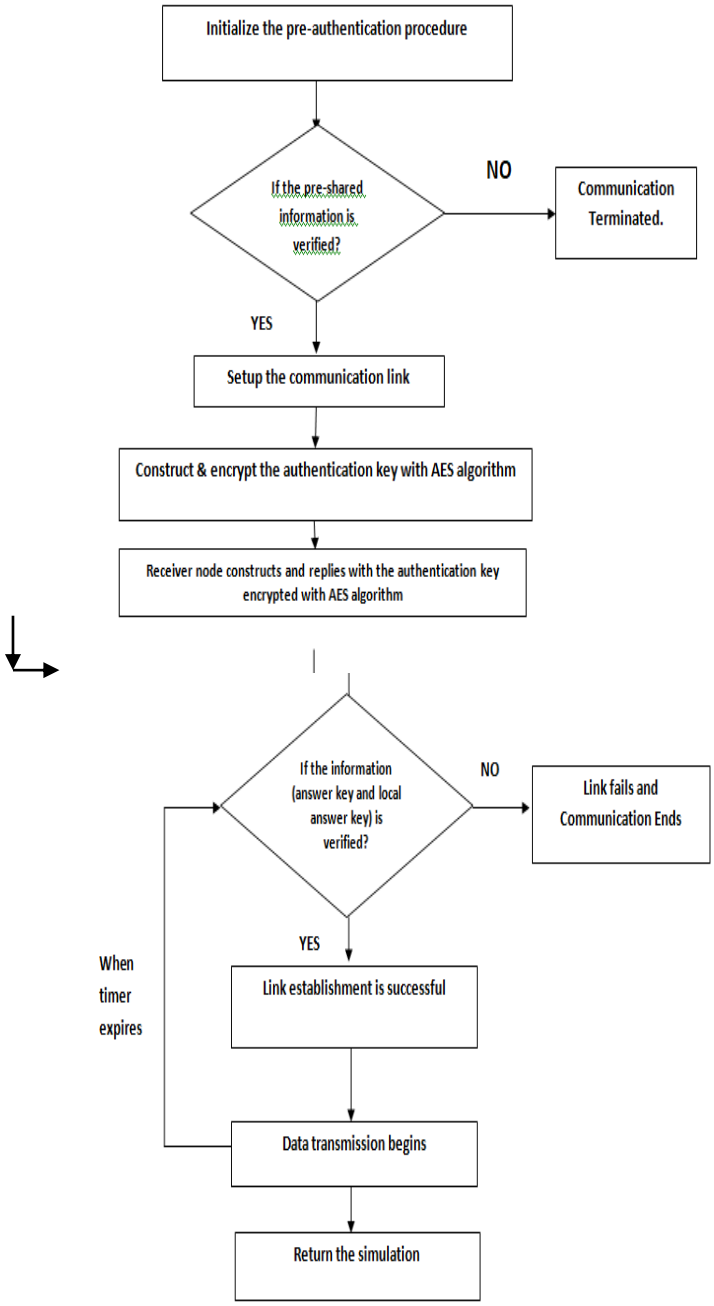

Figure 3:Detailed procedure of proposed IoT based authentication model

Proposed Algorithm

Algorithm 1: The proposed key management policy and algorithm design

Case 1: The sensor node to sink communication setup

1. The sensor node starts the establishment of the communication setup phase and place the request for the data transfer
2. The sink node starts the authentication method

Case 2: The peer-to-peer communication model

1. When sensor node receives the connection setup request from another node
2. The receiver node initiates the ready state and starts the authentication model
3. The receiver node starts the pre-authentication phase with the sender/requesting node.

Algorithm 2:

1. The base station infuses the multi-column keys to prepare the query key.
2. The query key is encrypted using the ECC algorithm.

3. The query key is forwarded to the mobile station.
4. The mobile station prepares the reply key by verifying the query key column data and marks the reply key rows.
5. The reply key is prepared by infusing the multiple keys information in the marked columns.
6. The reply key is encrypted using the ECC algorithm.
7. The reply key is forwarded towards the base station.
8. The base station verifies the query key against the reply and prepares the decision.
9. If the verification decision is successful
10. The call setup is complete and call is forwarded to the target mobile station.
11. Time counter (Tc) is initialized
12. Else
13. The call is dropped and the sensor node is informed about the authentication failure.
14. When the timer (Tc) expires, the exchange process is repeated.
15. If key verification is successful
16. The channel stays intact
17. Otherwise
18. The call is terminated

Algorithm 3: AES Algorithm Encryption Process

1. Input Image
2. Convert the image into Data Matrix (d)
3. Data Matrix Validation → validate(d) →d_M
4. Data Matrix Segmentation → segment((d_M) →d_m^i
5. Input Security Key (S_k)
6. Key Expansion(S_k)
7. Initial Round → Add Round Key (S_k)
8. Rounds → For Loop

a. Sub Bytes(d_m^i)
b. Shift Rows(d_m^i)
c. Mix Columns(d_m^i)
d. Add Round Key(d_m^i)

9. Rounds → End For Loop
10. Final Round → Mix Columns(*False*)

a. Sub Bytes(d_m^i)
b. Shift Rows (d_m^i)
c. Add Round Key(d_m^i)

11. Data Matrix Merger → merge(d_m^i) →dE_M
12. Data Matrix Reverse validation → revalidate($dE_{M)}$ →dE

IV. RESULT AND DISCUSSIONS

The proposed work has been done in MATLAB. The parameters required for simulation are listed in Table 1. The screenshot for building and encrypting key table is shown in Figure 4.

Table 1: Simulation Parameters

Network Parameters	**Values**
CPU	Intel Celeron 1.6 GHZ
RAM	4 GB
HDD	500 GB
Operating System	Microsoft Windows 7 (64-bit)
Software	MATLAB 2013 a
Programming Language	MATLAB

The results of the proposed scenario are obtained under the various experiments with different number of nodes, variable transmission range and constant energy transmission and receive values. In this scenario, 150 nodes are deployed randomly (using permutations) in the area of 200 x 200 square meter of flat ground area.

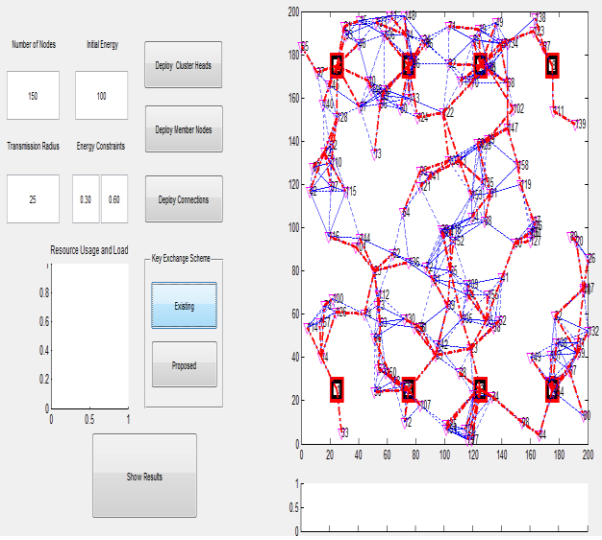

Figure 4:Working of IoT model on 150 nodes scenario

The energy of 0.30 and 0.60 milli-joules is used for the purpose of energy consumption estimation in the given scenario, which is tested for the 10 rounds of data sequence. The data is transmitted in 10 transmission events and the authentication is applied in all of the events to describe the effects of authentication on the data events during the authentication rounds. The proposed model has been analyzed for the projected resources over the given scenario of 150 nodes assigned with the transmission range of 25 meters. The proposed model consistently remains lower than the existing model on all of the data events in the following figure (Figure 5) for the projected resources.

The proposed model scenario is based upon 150 nodes, which are deployed randomly using the pseudo random number generation of the node coordinates. The projected resources for authentication are recorded between 5 and 10 percent for the proposed model, whereas in the existing model the project resources range lies between 7 and 20 percent. The proposed model consumed half resources in comparison with the existing model on an average in the 10 authentication/data events in the scenario with 150 nodes. The proposed model consumes the higher number of resources than the scenarios with 50 and 100 nodes, because it needs to host more number of authentication events per node than 50 and 100 nodes scenarios.

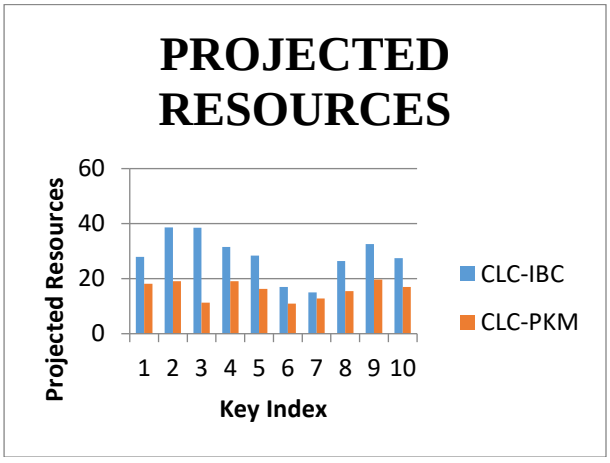

Figure 5:Analysis based upon the entropy with 150 nodes

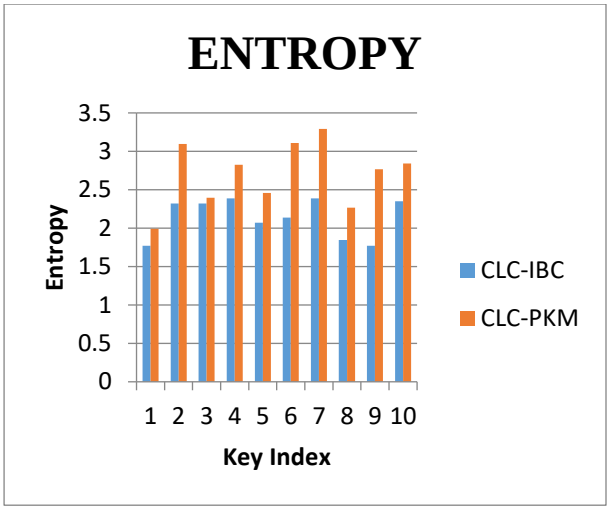

Figure 6:Analysis based upon the entropy with 150 nodes

The entropy of the proposed model has been recorded higher than 2 and below 3.5 on all of the data events in the given scenario. The proposed model has been found consistently higher than the existing model on all of the data events, which is clearly visible from the given scenario (Figure 6). The existing model is recorded between 1.7 and 2.4, which is considerably lower than the proposed model on all of the events.

The proposed model has been recorded with computational time in different scenarios with different number of nodes and varying transmission radius according to the number of nodes. The computational time trend is similar to the energy consumption and rising with rise in the number of nodes according to the following table (Table 2). Afterwards the average value of the computational time for all of the scenarios has been drawn in order to compare the proposed model's performance with the existing models.

Table 2:Computational Time of scenarios with different number of nodes

No. of Nodes	Computational Time (seconds)
50	0.04
100	0.09
150	0.16
200	0.29
250	0.53
Average	0.222

The proposed model has been recorded with the computational time of 0.22 seconds (Average of all scenarios), which is the lower value against all other readings. The CLC-IBC, MXH and YHZXZ schemes took 1.9 seconds, 4.05 second and 2.43 seconds respectively, which shows the robustness of the proposed model (Table 2).

Table 3: Computational time comparison with existing schemes

Scheme	Time(sec)
YHZXZ	2.43
MXH	4.05
CLC-IBC	1.9
Proposed	0.22

The following figure (Figure 4) describes the above table graphically for the results of computational time, which again justifies the similar trend as per shown in the table 5.10. The proposed model has been found efficient in comparison with all of the existing models as per shown in the following figure (Figure 4.8) in the

terms of computational time, which shows the rapidness of proposed model in handling the data traffic over the IoT networks.

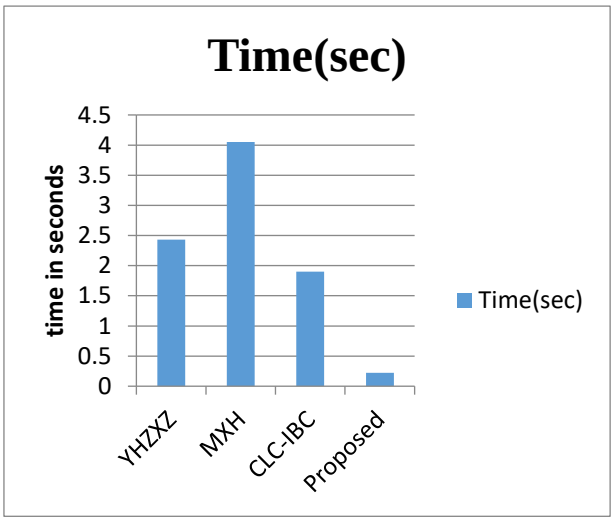

Figure 7:Computational time comparison with existing schemes

V. CONCLUSIONS AND FUTURE SCOPE

In this paper, the proposed model has been designed on the basis of paired key mechanism (PKM) for authentication along with advanced encryption standard (AES) cryptography for the enforcement of the security protocol over the internet of things (IoT). The multi-column complex key formation plays the vital role in the proposed model design. The set of algebraic functions are used for the formation of the complex keys over the multiple columns in the key table consisted of N rows and 8 columns. The paired key mechanism (PKM) based authentication uses the two sets of coefficients to produce the query key (columns 1 to 4, total 4 columns) and answer key (4 to 8, total 5 columns) from the key table using the cubic and quartic equation respectively. The experimental results show the average projected value of proposed model at 2.82, 13.218 and 28.337 against the 1.598, 2.523 and 15.962 of projected resources in the scenarios with 50, 100 and 150 nodes respectively. The experimental results show the average projected value of existing model at 2.82, 13.218 and 28.337 percent against the proposed model's 1.598, 2.523 and 15.962 percent of projected resources in the scenarios with 50, 100 and 150 nodes respectively. The comparison shows the average entropy of proposed model at 2.52, 2.82 and 2.71 percent against the existing model's 2.0, 2.13 and 2.13 percent of projected resources in the scenarios with 50, 100 and 150 nodes respectively. The results clearly shows the improved performance of proposed model over the existing model

VI. REFERENCES

[1] Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on (pp. 1-8). IEEE.

[2] Ali, S. T., Sivaraman, V., & Ostry, D. (2014). Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring. Future Generation Computer Systems, 35, 80-90.

[3] Bernabe, J. B., Ramos, J. L. H., & Gomez, A. F. S. (2016). TACIoT: multidimensional trust-aware access control system for the Internet of Things. Soft Computing, 20(5), 1763-1779.

[4] Hachem, S., Teixeira, T., & Issarny, V. (2011, December). Ontologies for the internet of things. In Proceedings of the 8th Middleware Doctoral Symposium (p. 3). ACM.

[5] Hernandez-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F., & Ladid, L. (2015). Toward a lightweight authentication and authorization framework for smart objects. IEEE Journal on Selected Areas in Communications, 33(4), 690-702.

[6] Hosseinzadeh, S., Virtanen, S., Díaz-Rodríguez, N., & Lilius, J. (2016, June). A semantic security framework and context-aware role-based access control ontology for smart spaces. In Proceedings of the International Workshop on Semantic Big Data (p. 8). ACM.

[7] Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. Procedia Computer Science, 34, 511-517.

[8] Kumar, A., Gopal, K., & Aggarwal, A. (2014, December). Simulation and analysis of authentication protocols for mobile Internet of Things (MIoT). In Parallel, Distributed and Grid Computing (PDGC),

2014 International Conference on (pp. 423-428). IEEE.
[9] Lee, J. Y., Lin, W. C., & Huang, Y. H. (2014, May). A lightweight authentication protocol for internet of things. In Next-Generation Electronics (ISNE), 2014 International Symposium on (pp. 1-2). IEEE.
[10] Lim, L., Marie, P., Conan, D., Chabridon, S., Desprats, T., & Manzoor, A. (2016). Enhancing context data distribution for the internet of things using qoc-awareness and attribute-based access control. Annals of Telecommunications, 71(3-4), 121-132.
[11] Peng, X., Zhang, H., & Liu, J. (2014). An ECG Compressed Sensing Method of Low Power Body Area Network. Indonesian Journal of Electrical Engineering and Computer Science, 12(1), 292-303.
[12] Xu, G., Cao, Y., Ren, Y., Li, X., & Feng, Z. (2017). Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things. IEEE Access, 5, 21046-21056