FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 264-269 | e-ISSN: 2347-470X

An Advanced and Efficient Cluster Key Management Scheme for Agriculture Precision IoT Based Systems

Sakshi Anand[1] and Avinash Sharma[2]

[1]PhD Scholar, CSE Department, M.M. Deemed to be University, Mullana, Haryana, India, sakshi.girdhar.1@gmail.com
[2]Professor, CSE Department, M.M. Deemed to be University, Mullana, Haryana, India, asharma@mmumullana.org

*__Correspondence:__ Avinash Sharma; Email: asharma@mmumullana.org

ABSTRACT- Things that connect to other devices & systems via Internet or communication networks are called IoT. It can also be said as a network of wireless sensors connected to a cloud and controlled by embedded devices. Considering the large framework of IoT, it becomes a little difficult to maintain security at each sensor node especially with limited information regarding hardware and deployment capabilities. Therefore, management of keys has become a point of concern peculiarly taking account of node capturing attack. This paper proposes an advanced cluster key management scheme for agriculture precision which involves EBS constructor and Chinese remainder theorem together. Once the data is collected from the nodes and a list is created, it is sent from the Cluster Head to the Backend Server, which filters it for hostile IDs and ignore the unauthentic sensor, returning filtered list with preloaded keys, & an authentication code to Cluster Head for use. To ensure added security, in this scheme encryption of data is done twice. Upon comparing the proposed scheme with others, it has been observed that we have achieved higher delivery ratio and reduced the energy consumption and packet drop rate to a great extent.

Keywords: IoT, Clustering key management, Agriculture precision and WSN, key management.

ARTICLE INFORMATION
Author(s): Sakshi Anand and Avinash Sharma
Received: 02/05/2022; **Accepted**: 11/06/2022; **Published**: 20/06/2022;
e-ISSN: 2347-470X;
Paper Id: IJEER220500;
Citation: 10.37391/IJEER.100235
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100235.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Increasing number of industries are turning to the IoT to improve their productivity and efficiency. Internet of Things security issues, including data theft and unlawful access, must be guarded against in sensors, smart devices and embedded devices [1]. It is possible to improve yields and prevent crop damage owing to the Internet of Things by using improved sensors in aerial vehicles (such as agricultural drones etc.). A further usage of IoT may be found in hydroponics & small-scale aquaponic systems too. In order to handle agricultural data utilizing big data technologies, several companies have designed platforms for monitoring plant health and making suggestions based on data specifically targeting agricultural IoT use cases [16].

1.1 IoT: Need and Characteristics

The usage of sensors and other IoT devices in agricultural, infrastructure, and home automation has prompted several enterprises to embark on digital transformation efforts as well, despite their widespread use in manufacturing, transportation, and utility companies [2]. In order to offer humans with a safe and comfortable way of life, the IoT aspires to link all possible things to the internet. It is feasible to have a linked world because to the IoT.

The usage of IoT applications is growing in variety of industries, counting agriculture, transportation, electric power, & city/home automation [3]. As the Internet of Things has created security flaws like data theft and unauthorized access to devices like sensors and smart gadgets it requires a defensive mechanism in order to combat them. *Figure 1* shows some of the general characteristics of IoT such as connection, communication, intelligence etc.

a. **Things**: are the objects that are capable to be connected as it has been developed for connection. Usually, sensors and household appliances are connected to livestock. These have the ability of sensing and perform as per circumstances.
b. **Data**: The basic idea of engaging and making use of devices via internet is centred on the term data. The interconnected sensing nodes transfer data after capturing for decision making. Actions are performed as per data based on a stored program that is making devices more intelligent.
c. **Communication**: Io T devices are connected in such a way that they could transfer information and this information might be analysed. Data transmission might be performed over small distances. Data could also be communicated over a large distance. E.g., Wireless Fidelity, LPWA (Low Power Wide Area) networks such as LoRa (Low Range Radio) or NB-IoT (NarrowBand-IoT).
d. **Intelligence**: IoT devices sense the information and perform the smart operation. This makes the IoT mechanism intelligent. An intelligent mechanism allows the IoT device to perform big data analytics
e. **Action**: It is known as step taken or task performed by intelligent system. Action might be manual as well as automated. Dependence of Action is on smart decisions specified by intelligent system.

f. **Ecosystem**: This is the location of IoT. Ecosystem considers technologies, objectives and concept at which Internet of Things is working.

g. **Connection**: This term does not require much explaining. The IoT devices are sensor-based and such pieces of equipment have been connected to the internet. The hardware as well as application plays a significant role in using IoT devices efficiently.

1.2 IoT & Agriculture

Precision agronomy employs IoT technology most often for precision farming. Smart cities often make use of SDNs (Software-Defined Networks) and CPSs (Cyber Physical Systems). Because of the Internet of Things, drones, such as agricultural drones, may assist farmers increase crop yields. Another IoT use is aquaponic & hydroponic systems, both of which employ IoT. Intelligent greenhouses are becoming common in urban areas due to their capacity to monitor several nutrient solution parameters and improve plant growth, productivity, and quality. Cities that have infrastructures that allow for automated, optimised, and enhanced urban agriculture and precision agronomy would profit immensely from these advancements. Another example of IoT technology in action is the ability to monitor and adjust the moisture and water content of soil. One more IoT-AI example is Malthouse, an artificial intelligence system used in the precision agriculture and food production sectors.

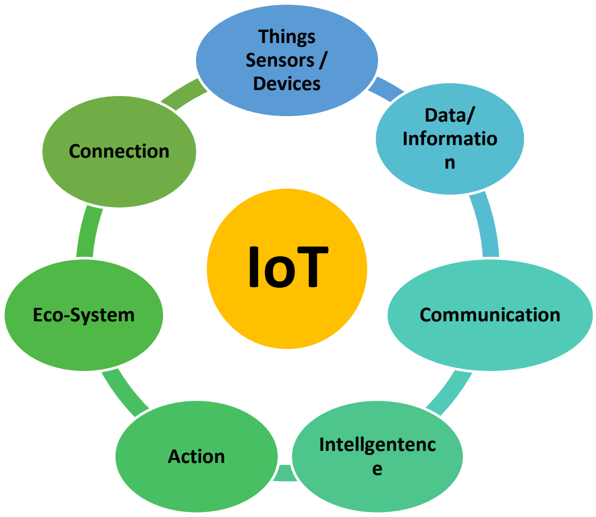

Figure 1: Characteristics of IoT

1.3 Agriculture Precision

It is use of innovative technology & field data. It focuses on data gathering, analysis, and variable rate input application. Also, the Internet of Things is reshaping several facets of human existence. It is paradigms that may employ IoT benefits to increase production efficiency, improve crop quality, and reduce environmental impact. Precision agriculture using Wireless Sensor Networks (WSNs) improves overall efficiency, production, and profitability. WSNs are critical components of the IoT, which allows users to access data from practically anywhere in the globe. Among the many benefits that IoT offers, its capacity to revolutionize present farming practices is truly groundbreaking [7]. Most concepts involve WSN that collects data from multiple field sensors and transfers it to a central server. This strategy studies environmental elements to increase agricultural productivity.

1.4 Wireless Sensor Network (WSN)

The development of wireless sensor networks (WSN) is increasing at an accelerating rate around the world. This is the initial consideration for any network security solution for communication devices [14]. Sender nodes authenticate messages by encrypting them with safe keys then encrypting them again. The adversary can readily discover a key compromise across the entire network when using a single key-based key management system, notwithstanding the simplicity and efficiency. As a result, to ensure the safety of sensor networks, multiple key-based schemes are employed [4]. WSN makes use of a number of important distribution strategies. It is possible to disseminate the key prior to putting nodes in place in the working field. These secret keys can be used by nodes to communicate with one another. Pre-distributed keys have 3 phases:

- establishment of path key,
- key generation and initialization
- key discovery

The keys work in this order: When nodes share similar keys & communicate via these links, a hidden path is constructed. The keys are selected at random from the pool of available keys in the pre-distribution procedure.

1.5 Cluster Based Key Management System (CBKMS)

For WSN, a key management mechanism is needed to address security concerns [5]. As a result, implementing a security solution is more difficult in an abandoned setting where sensors are more likely to be targeted. In CBKM, sensors and the CH (Cluster Head) communicate with each other just once. Using the Cluster Head BS, a unique id, Pairwise Key, and unique group key are generated and preloaded into the network sensors before they are sent to the cluster. Every few minutes, CH transmits a message to all nodes that contains the group keys for all nodes. In the join request message, they submitted previously, nodes send back their encrypted IDs and group keys. An ID list is generated and sent from CH to the BS (Backend Server). The BS filters the list by looking for hostile IDs and disregarding the unauthentic sensor, then sends it back to CH with pre-loaded keys, & message authentication code. Each time CH delivers a packet to the BS, this number is incremented to verify the currency of the message. The sensor IDs, & substitute message will be sent back to the user via CH. A pair-wise key has been used to encrypt this message. This technique therefore creates a secure environment for node movement, but it is important to limit cluster mobility in order to ensure energy availability while also increasing throughput. [6] Because the cluster head interacts directly with each node, the node compromise may be minimized.

2. LITERATURE REVIEW

The focal point of this study of agriculture precision was attained after studying research works on varied topics including IOT, Clustering key management, Agriculture precision and WSN. The purpose of different researches was to determine distinct WSNs technologies that are employed in precision agriculture and their influence on smart farming. Some researches show concerns in selecting an efficient key management scheme because of issues such as memory restrictions and energy constraints also power consumption of various wireless communication technologies was compared based on usual communication time in one of the papers.

The general research was focused mostly on clustering algorithms in order to identify clustered methods based on grouping and distribution of keys during communication. A paper organized the network in clusters that were groups of nodes being maintained and reassembled employing specialized algorithms and approaches. Moreover, they made use of request suppression in the clustered strategy to limit the number of responses for the searching process.

3. PROPOSED WORK

3.1 Cluster Formation

Cluster heads are selected in WSN after nodes have been distributed in environment and before the base station has received their positions. If a node is competent enough of officiating as a cluster head, the capability of that node to be selected depends on factors such as communication range, processing capacity and energy resources as per the algorithm. Encryption is used during the authentication procedure to provide security.

If a node meets the selection requirements, it has the ability to lead the cluster. The Cluster head beacon (CH BEACON) packet is emitted by this node, Nb. Key *Kp* is used to encrypt the CH BEACON packet, which is known as the main key. *Nb* will receive a Cluster Head REPLY (CH REP) message from the nodes that are interested in joining the cluster when they get this message from *Sb*. There is an ID and response content in the reply message. As long as the number of replies received by *Nb* exceeds a certain threshold P^{th}, the cluster head, CH, may be picked by Nb. Last but not least, the nodes that will join the cluster are given IDs by the cluster leader.

3.2 EBS (Exclusion Basis System) Construction

The member set collection is divided into many subsets to form an EBS (Exclusion Basis Systems). Each subset in the EBS may be compared to certain key, & nodes that have that key are subset's elements. N, K, M is the dimension of the EBS, which illustrates the state of a strong group with members numbered from 1 to N and each subset has unique key, K being the number of keys with each element of group and number of rekey messages are represented by M. Every member of subset Ai in EBS will have access to the key Ki. For any t € [1, N], EMS has M elements, and the union of these elements is equal to [1, N]. A member t may thus be expelled from the key server. The replacement keys for the K keys are then re-keyed so that each member is aware of the new keys.

Following the encrypting process, the M messages are broadcast using the keys that correspond to M elements. Every key is encrypted by the one before it in order to limit the number of people who can decode it.

To create EBS subsets, we employ a canonical enumeration approach. When deciding which *K+M* items to include in a subset of *K*, every possible technique is taken into account. The "canonical matrix" of EBS (N, K, M) is matrix *A*, which is used to construct a bit string sequence in which *M* and *K* are known. The C columns represent subsequent bit strings, each of which has length of *M* + *K* objects.

For the purpose of creating a higher number of management keys in this protocol, N, K and M are increased during the EBS model generation. For cluster's new nodes, spare keys are utilized.

3.3 Advance Efficient Cluster Key Management System (AECKMS)

It is possible to lower the cost by using EBS and the Chinese remainder theorem in conjunction. The EBS framework is utilized to manage the group key computation in this system using a combinatorial formulation. There are three variables that govern how many keys each member has and how many rekeying messages each member receives. For n users, this method yields an arrangement somewhere between m and k. They have an administrator key *(k+m)* that they may use. *c(k+m,k)* denotes the total key. There are k keys for each member of the group. Once the base station is aware of the sensor's actual position, the sensor is free to choose their own CH. The sensors then transmit their IDs to the associated CH, which in turn transmits data acquired to the BS. Chinese remainder theorem is used to produce secret information K with the use of these facts. After that, it's sent to all of the cluster's nodes, one by one, through each CH.

A total of 100 sensor nodes were randomly placed in a 1000 X 1000m area. At the distance of 100 meters from the specified area, two sink nodes are located. Channel capacity for mobile hosts in the simulation is set at 2 Mbps. UDP is used to imitate CBR traffic. There are a total of nine clusters produced. Data from four cluster heads is sent to the sink. Each cluster head receives data from three sensor nodes. Intruder nodes range from two to ten. Figure 2 presents proposed model; here sensor nodes are connected to base station that is transferring information to server and precision agriculture which is connected to energy efficient cluster key management for IoT based systems.

A generalized equation used in the proposed scheme defines precision, recall, accuracy and f1-score.

Precision = true positive / (true positive + false positive)
Recall value= True positive / (True positive + False negative)
Accuracy = (True positive + True negative) / (True positive + False positive + True negative + False Negative)
F1-score = 2TP /(2TP +FP +FN)

In terms of performance, I have compared the proposed scheme, Advanced and Efficient Cluster Key Management Scheme (AECKMS) with SecLEACH (Secure low-energy adaptive clustering hierarchy) and EECBKM (Energy Efficient Cluster Based Key Management) strategy. Following measures are used to assess performance.

- Assuming all data packets reach their final destination, the average number of packets lost as a result of various assaults is called "average packet drop."
- As a measure of how many packets are successfully delivered, the average delivery ratio is calculated by dividing several packets received by total packets sent.
- As a general guideline, data transmission uses an average amount of energy.

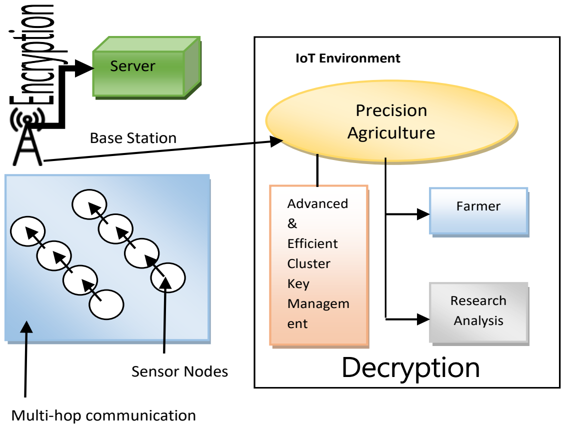

Figure 2: Proposed Architecture

4. RESULT AND DISCUSSION

4.1 Case Consideration

The simulation for cluster head selection has been made in MATLAB R2020A environment where file handling, plotting and image processing tools are used. Here multiple cases are considered case 1 is considering 25 nodes *(Figure 3)* whereas case 2 considered 50 nodes (*Figure 4*), case 3 has considered 75 nodes (*Figure 5*), case 4 presented 100 nodes (*Figure 6*Figure 6*)*.

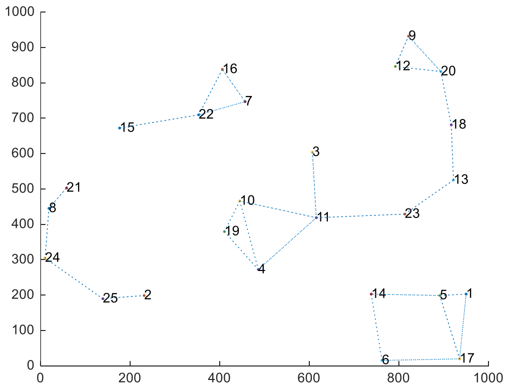

Figure 3: Cluster Head in case of 25 nodes

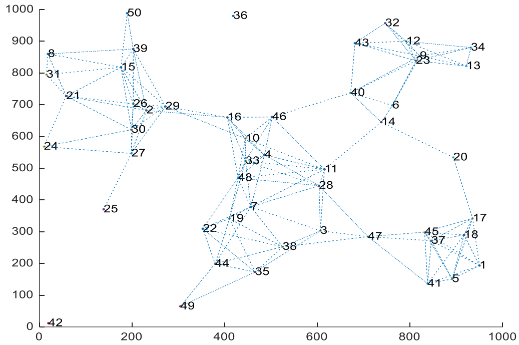

Figure 4: Cluster Head in case of 50 nodes

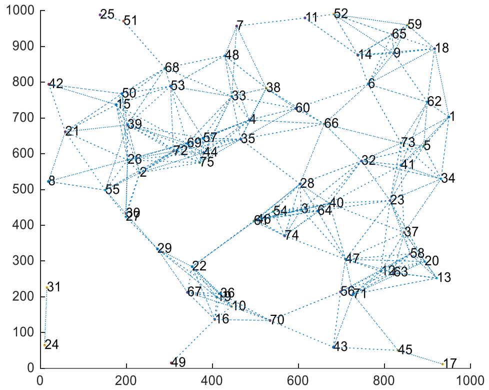

Figure 5: Cluster Head in case of 75 nodes

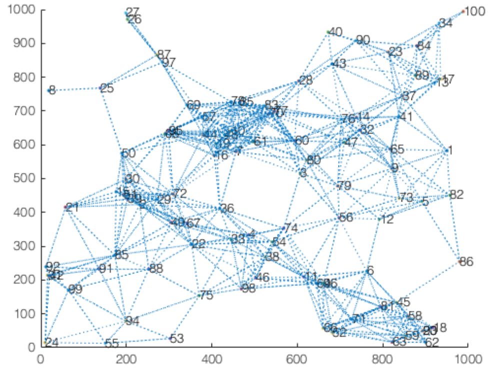

Figure 6: Cluster Head in case of 100 nodes

4.2 Based on Attackers

Increasing the number of attackers will naturally lead to an increase in packet loss, resulting in a decrease in packet delivery. Compared to current systems, AECKM decreases node capture attacks, which lowers packet loss. When several attackers is greater than before, packet delivery and drop ratio are shown in *Figures 6 and 7*.

Node capture attempts were carried out by 2, 4, 6, 8, and 10 attackers from distinct clusters in our first experiment and a comparison with other schemes is made in *Table 1* and *Figure 7* with respect to attackers and Delivery ratio, *Table 2* and

Figure 8 with respect to attackers and Packet Drop and *Table 3* and *Figure 9* with respect to attackers and Energy consumed.

Table 1: Attacker Vs Delivery Ratio

Attackers	EECBKM [11]	SecLEACH	Proposed work
2	0.444	0.439	0.445
4	0.443	0.438	0.510
6	0.442	0.435	0.456
8	0.441	0.431	0.460
10	0.4405	0.43	0.486

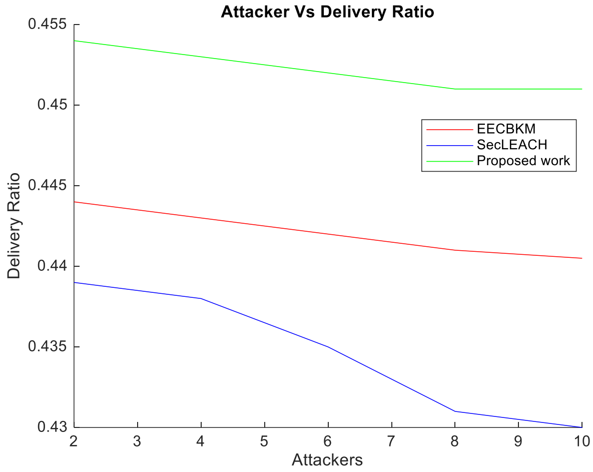

Figure 7: Attacker Vs Delivery Ratio

Table 2: Attackers Vs Drop

Attackers	EECBKM[11]	SecLEACH	Proposed work
2	21100	23000	21028
4	21000	23000	21000
6	21010	23000	20922
8	21020	23500	20995
10	22000	23800	21953

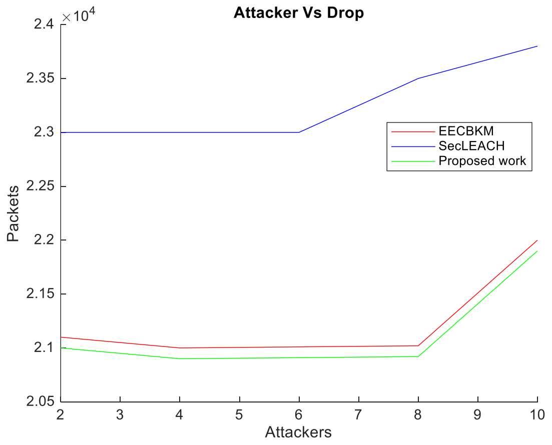

Figure 8: Attackers Vs Drop

Table 3: Attackers Vs Energy

Attackers	EECBKM [11]	SecLEACH	Proposed work
2	14	16	13
4	14	16	13
6	14	16	13
8	14	16	13
10	14	16	13

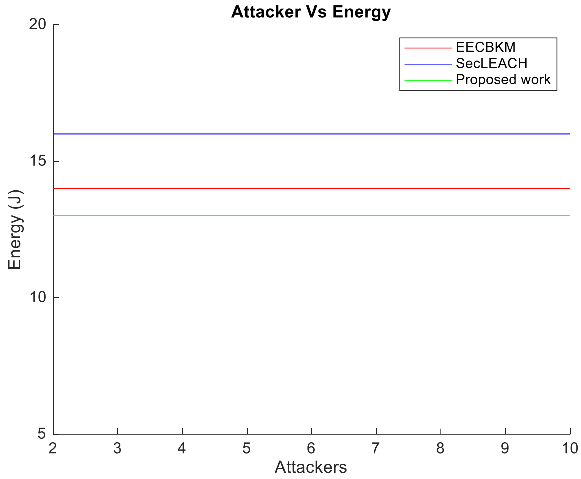

Figure 9: Attackers Vs Energy

5. CONCLUSION

The proposed work has simulated reliable and energy efficient cluster head key management system for IoT based agriculture precision. After simulation it has been concluded that delivery ratio in case of proposed work is more as compare to previous research work. On other and proposed work is having less drop rate and energy consumption. In this way proposed work is better as compared to previous works.

6. SCOPE OF THE RESEARCH

For small farms, precision agriculture may aid with sub-surface drip irrigation for accurate water and fertilizer delivery and robots for weed control, harvesting and other tasks. With WSNs, precision agriculture increases overall efficiency, productivity, & profit. In other words, Precision agriculture may help small farms with sub-surface drip irrigation for precise water and fertilizer delivery, as well as robots for weed control, harvesting, and other activities. Precision agriculture is more efficient, productive, and profitable thanks to Wireless Sensor Networks (WSNs).

REFERENCES

[1] Kumar, V., Malik, N., Dhiman, G. and Lohani, T.K. (2021), "Scalable and Storage Efficient Dynamic Key Management Scheme for Wireless Sensor Network", edited by Shanmuganathan, V.Wireless Communications and Mobile Computing, Vol. 2021, pp. 1–11.

[2] Anand, S. and Sharma, A. (2021), “Hybrid Security Mechanism to Enhance the Security and Performance of IoT System”, IEEE Xplore, 1 December.

[3] Yadav, C., Yadav, V. and Kumar, J. (2021), “Secure and Reliable Data sharing scheme using Attribute-based Encryption with weighted attribute-based Encryption in Cloud Environment”, International Journal of Electrical and Electronics Research, Vol. 9 No. 3, pp. 48–56.

[4] Gulzar, B. and Gupta, A. (2021), “DAM: A Theoretical Framework for SensorSecurity in IoT Applications”, INTERNATIONAL JOURNAL of NEXT-GENERATION COMPUTING, Vol. 12 No. 3, available at: https://doi.org/10.47164/ijngc.v12i3.830.

[5] “Energy Efficient Cluster-Based Routing Protocol in Wireless Sensor Network using Flower Pollination Algorithm | IJEER”. (n.d.). Ijeer.forexjournal.co.in, available at: http://ijeer.forexjournal.co.in/archive/volume-4/ijeer-040308.php.

[6] Mehmood, G., Khan, M.S., Waheed, A., Zareei, M., Fayaz, M., Sadad, T., Kama, N., et al. (2021), “An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network”, edited by Volchenkov, D.Complexity, Vol. 2021, pp. 1–10.

[7] Kumar, V. and Choudhary, A. (2021), “Solar Water Pumping Model Using Zeta Converter for Irrigation Application”, International Journal of Electrical and Electronics Research, Vol. 9 No. 3, pp. 84–88.

[8] Liao, B., Ali, Y., Nazir, S., He, L. and Khan, H.U. (2020), “Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review”, IEEE Access, Vol. 8, pp. 120331–120350.

[9] Jia, C., Ding, H., Zhang, C. and Zhang, X. (2021), “Design of a dynamic key management plan for intelligent building energy management system based on wireless sensor network and blockchain technology”, Alexandria Engineering Journal, Vol. 60 No. 1, pp. 337–346.

[10] Susan T, S.A. and Nithya, B. (2020), “Cluster Based Key Management Schemes in Wireless Sensor Networks: A Survey”, Procedia Computer Science, Vol. 171, pp. 2684–2693.

[11] Li, J., Wu, J., Chen, L., Li, J. and Lam, S.K. (2021), “Blockchain-based Secure Key Management for Mobile Edge Computing”, IEEE Transactions on Mobile Computing, pp. 1–1.

[12] Basile, M., Dini, G., Vernia, F. and Lamoglie, L. (2020), “A Secure and Efficient Group Key Management Scheme for Clusters of String Inverters”, Applied Sciences, available at: https://agris.fao.org/agris-search/search.do?recordID=DJ20210339955.

[13] Apsara, M.B., Dayananda, P. and Sowmyarani, C.N. (2020), “A Review on Secure Group Key Management Schemes for Data Gathering in Wireless Sensor Networks”, Engineering, Technology & Applied Science Research, Vol. 10 No. 1, pp. 5108–5112.

[14] Anand, S. and Sharma, A. (2020), “Assessment of security threats on IoT based applications”, Materials Today: Proceedings, available at: https://doi.org/10.1016/j.matpr.2020.09.350.

[15] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. (2019), “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures”, IEEE Access, Vol. 7, pp. 82721–82743.

[16] Anand, S. and Sharma, A. (2019), “Internet of Medical Things: Services, Applications and Technologies”, Journal of Computational and Theoretical Nanoscience, Vol. 16 No. 9, pp. 3995–3998.

[17] Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P. (2019), “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved”, IEEE Internet of Things Journal, Vol. 6 No. 2, pp. 1606–1616.

[18] Robinchandra Singh, U. and Roy, S. (2019), “Survey on Key Management Schemes and Cluster based Routing Protocols in Wireless Sensor Network”, Papers.ssrn.com, Rochester, NY, 22 March, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3358290.

[19] Anand, S. and Sharma, A. (2019b), “Issues and Concerns in Security of Cloud Environment in Internet of Things”, Journal of Computational and Theoretical Nanoscience, Vol. 16 No. 10, pp. 4374–4378.

[20] Chen, L. (2017), “Security Management for The Internet of Things”, Electronic Theses and Dissertations, available at: https://scholar.uwindsor.ca/etd/5932/.

[21] Corser, G. (2017), Internet of Things (IOT) Security Best Practices, available at: https://standards.ieee.org/wp-content/uploads/import/documents/other/whitepaper-internet-of-things-2017-dh-v1.pdf.

[22] Jawad, H., Nordin, R., Gharghan, S., Jawad, A. and Ismail, M. (2017), “Energy-Efficient Wireless Sensor Networks for Precision Agriculture: A Review”, Sensors, Vol. 17 No. 8, p. 1781.

[23] Riahi Sfar, A., Natalizio, E., Challal, Y. and Chtourou, Z. (2018), “A roadmap for security challenges in the Internet of Things”, Digital Communications and Networks, Vol. 4 No. 2, pp. 118–137.

[24] Hemapriya, K. and Gomathy, K. (2007), “IJARCCE A Survey Paper of Cluster based Key Management Techniques for Secured Data Transmission in Manet”, International Journal of Advanced Research in Computer and Communication Engineering ISO, Vol. 3297, available at: https://doi.org/10.17148/IJARCCE.2016.510102.

[25] Zhao, Q. and Liu, X. (2014), “Cluster Key Management Scheme for Wireless Sensor Networks”, Www.atlantis-Press.com, Atlantis Press, 1 May.

[26] Bao, X., Liu, J., She, L. and Zhang, S. (2014), “A key management scheme based on grouping within cluster”, IEEE Xplore, 1 June.

[27] Lalitha, T. and Umarani, R. (2011), “Energy Efficient Cluster Based key Management Technique for Wireless Sensor Networks”, Www.semanticscholar.org, available at: https://www.semanticscholar.org/paper/Energy-Efficient-Cluster-Based-key-Management-for-Lalitha Umarani/6721f474204f198be38226eebdde5c5d691368ba.