Journal of Advanced Zoology
ISSN: 0253-7214
Volume 45 Issue S-4 Year 2024 Page 55-64

# Understanding Cyber Security In Health Sector

**Dr. Janardan Pawar[1*], Dr. Dhanashri Kulkarni[2], Valmik Dhanwate[3]**

*[1*,2,3]Indira College of Commerce and Science, Pune, Maharashtra.*
*Email: janardanp@iccs.ac.in[1], dhanashriskulkarni05@gmail.com[2], valmik.dhanwate@iccs.ac.in[3]*

***Corresponding Author:** Dr. Janardan Pawar*
**Indira College of Commerce and Science, Pune, Maharashtra. Email: janardanp@iccs.ac.in*



***Abstract***

Digital attacks include extorting money from users, altering, destroying, or gaining access to sensitive data, stopping regular business operations, and more. The medical and health sectors offer numerous potential for cyber security. Digital assaults can take many different forms, such as extorting money from users, destroying, altering, or accessing sensitive material in question areas, interfering with regular corporate operations, etc. Cybersecurity has various prospects in the health and medical sector. This research investigation's main goal is to concentrate safe practices in specific industries. It is very necessary starting with the second generation of computing and will continue to be so till there are computers and data in the digital realm. The medical fields of today also use digital communication and documentation. Such documents must be protected at the highest possible priority. As healthcare systems have delicate information, it becomes essential to protect such sensitive information from cyber threats. In smart healthcare systems, the patient's information is periodically collected and transmitted seamlessly to the decision-making system. However, protecting such sensitive data transmission from cyber threats becomes a challenging research problem at the edge layer. This paper addresses the challenges of cyber-attack and this study is greatly applicable for health sector.

***Keywords:*** **Cyber Security, Medical, IOT, Medical, Artificial Intelligence.**

## I. INTRODUCTION

Concerns about breaches of personal data in the medical industry have grown in the last few days. Compared to the finance sector, security arguments in the health care industry are receiving less attention; nonetheless, medical data is nonetheless extremely important and sensitive [1] expressed that cyber-attacks were become the consistent reasons of health-care data gaps. Medical institutions gather and save the patients data on their systems in databases, for example, those on their sites, electronic medical recording (EMR) systems, order communication systems (OCS), and picture archiving and communication systems (PACS); consequently, information security is firmly connected to cyber-security [1- 6]. Additionally, if medical data is not confidential, there will be the adverse consequences, like patient's data leakage, patient's misdiagnosis and mistreatment. This leads to a serious effect on the physical and psychological health of the patient. As the increased living standards of people makes the more demand for the betterment in the medical systems. [7]

have designed a mobile smart medical system and made an analysis of potential attacks on it [8] has proposed a medical system taking into consideration of multi-lifecycle environment. This system mainly focusses on medical equipment's rather than the web applications. This system makes an analysis and improvements on the lifetime of medical equipment's, so that the patient can be given with a batter medical health-care. With the help of a medical system and good network techniques, we focus on cyber-security and its impacts in the medical domain [9] presented their research work on medical process with Internet-of-Things (IoT) technology. They have obtained that the IoT has the capability in the reduction of treatment time and can improve the treatment efficiency [1][10] have implemented a supervisory exchange method that keeps the medical system stable and improves the safety level.

This research work presents an overview of dataflow in the medical domain. Also, we identify the vulnerabilities present in the different stages of dataflow. Next, the weaknesses are identified accordingly, the classification techniques for the cyber-attacks were presented. Also, this work presents the additional research on previous work that focuses on solving these cyber-attacks and identifies the strengths and limitations of the solutions of various cyber-attacks. For the data storage assurance, also we have discussed the various cyber-security models for the medical domain. It was observed that the counter-measures from previous works and models are weak with respect to resource depletion, attack reduction, applicability, etc. Finally, we present the effective models relevant to protection of medical data against these cyber-security vulnerabilities and attacks.

## II. REVIEW OF LITERATURE

When it comes to networking of any kind, name and addressing are necessary components. Because routing protocols need name and addressing to convey data to sensor nodes [86]. To prevent any confusion, each node is given a specific, one-of-a-kind name or address that is referred to as its identity. Services need names so that they can be identified, discovered, and used, and routing systems require addresses so that they can route packets.

Identity theft may lead to several attacks, including the Sybil attack and the node replication assault, which target name and addressing methods. Identity theft occurs when an illegitimate node already has an address given to it and is utilising it, but an adversary starts using that address instead. The term Sybil attack refers to a situation in which a single malicious node tricks other, genuine nodes into thinking there are many other nodes in the area by using multiple fabricated addresses. The node replication assault is the counterpart of the Sybil attack [23].

The adversary finds it straightforward and inexpensive to conduct a node replication assault since this kind of attack does not need the compromise of many nodes. The major expense is in collecting and altering a single sensor, then duplicating the altered sensor to create several copies [98]. Furthermore, knowing merely the topology in a small area is insufficient to spot a clone. Since a sensor's communication architecture only provides limited topological information, detecting such an attack is very difficult (originally). Specifically, a node replication assault is a risky attack because it allows an adversary to quickly destroy the primary objective of the deployed network by deploying many replica nodes. An identity theft-based NRA is the focus of this thesis.

### a. SECURITY SCHEMES

Ideal security architecture [22] includes measures for prevention, detection and recovery. Preventive measures that prevent the attackers from tampering with communication messages, e.g., like encryption and authentication. Detective measures that perform anomaly detection during protocol executions and alerts when it exceeds certain tolerance level. Reactive measures that cause work around to the attacks, or even initiate counterattacks. A well-known classification of the security strategies for classical computer systems is: (i) Prevention, (ii) Detection, and (iii) Recovery.

#### PREVENTION MECHANISMS

Provide the mechanisms to prevent the easy access of sensor components as well increase the effort required to study the stored data by the adversary or increasing the effort taken to compromise the node.

Provide mechanisms to defeat the node compromise made by the adversary such that the cryptographic keys stored in a sensor node must be protected.

#### DETECTION MECHANISMS

Provide Mechanisms to detect spoofed data is an alternate way of detecting compromised node in En-route filtering schemes.

To detect replicated node/ node compromise by location verification scheme and code testing strategies. Code testing schemes are based on the approaches are software, hardware, trusted platform module. Software-based code attestation uses hash values of randomly selected memory areas to verify sensor node memory and optimise programme verification [23].

**RECOVERY MECHANISMS**

The first form recovery mechanism is to stop an attack and fix any damage caused by the attack. Here, the system's functionality is suppressed by the attack and continuation of correct operation is required. Another form recovery is the system remains to function correctly though an attack is happening. It is usually used in safety-critical systems and depends on fault tolerance. The following four kind of mechanism which employ any of the forms of recapture recognized as to exclude, to reprogram, to adopt, and to tolerate the compromised node [23]:

- TO EXCLUDE - Continuation of Attack by an adversary can be stopped by omitting from any further participation of the compromised sensors nodes in the network [76].
- TO ADOPT (WITH THRESHOLD) – Compromised node allowed to participate in the network until he has not cooperated again more than the threshold value [23*]*.
- TO REPROGRAM (COMPROMISE) - The sensor nodes may require reprogramming either to increase security features, or to remove malicious program from the compromised nodes [23][38].
- TO TOLERATE NODE COMPROMISE- WSN functionalities remain same until the number of node compromise less than threshold by the adversary. This method also considered to be preventive action. Sometimes extra action may be needed [23].

**b. NODE REPLICATION ATTACK DETECTION MECHANISMS**

This is the most recent revision of the taxonomy that is presented in [23]. Both centralised and distributed systems have the same overarching goal, which to have points make location claims that show where they are and seek to discover contradicting report(s) that show the same node in various places [12][45]. Because of this, it is necessary for sign each node and transmit a position privilege, as well as verify and retain the signed location claims of all other nodes [11][14]. The sections that follow will provide an overview of the several detection methods currently in use for replication attacks.

Because centralised detection techniques have a SPOF, the distributed detection strategy has greater advantages than centralised detection approaches. Randomness is introduced while picking witnesses at different levels, such as the full network, and is confined to geographical grids in the witness-based strategy of distributed systems. This is done to prevent the what future witnesses will say [13]. If the selected witness point was itself a negotiated point or a replicated point, then the identification of a duplication occurrence would be questionable [12][13][16]. Certain WSN applications require transportable nodes [13]. The total procedures became more complicated when mobile nodes are taken into consideration [12][13][19][40][46]. Mishra & Turku broadly classified the ways to find out about NRA in WSN is by as centralized, partially distributed and fully distributed based on the nature of detection mechanism [24][34]. And also they classified location dependent and location independent based on the geographical information. Further classification done based on claim forwarding strategy and message routing method. Deterministic and probabilistic forwarding is categorized under claim forwarding strategy. Link based and geographical routing schemes under the category of message routing. The subsequent subsections will describe various existing centralized detection schemes for NRA.

A technique for detection that is based on an area is presented in health care [30]. According to their plan, the central node will be chosen from among the nodes based on the highest number of neighbours each has. After then, the whole network is divided up into smaller sections called sub-areas. Every sub-region is situated in the exact same location around the head node. A witness node is chosen in each subarea using procedures that are like those used for choosing the central node. Now, before beginning communication with other nodes, the source node must first communicate its location-claim to the witness node for its sub-area. It notifies every node in the network of any conflicts that it finds or that arise, and it does this by broadcasting the information. If this is not the case, the witness node will transmit these claims to the central node of the region for further replica detection at the network level. The purpose of this is to identify keys that can be used on cloned nodes by keeping track of how often they are used are used to authenticate the node in the network [12][13]. The reasoning behind this is as follows: In this scenario, every node performs a screen that counts blooms on the keys that are issued to interact with the nodes that are nearby, and then appends its own count to the result [12][13]. After that, the bloom filter and count are transported into the base station, where it will be recognised based on the count the number, also known as how many times each key in the network is used [12][13]. It is

possible to see the key use as suspicious if it goes over and beyond the limit. In the protocol, each node was responsible for communicating the key information to its own base station. After that, the base station would use a combination of mathematical and computational methods to search for duplicated keys [16][40][47]. Broadcasting from one node to another in a network, using a witness selection approach, and being knowledgeable about deployment are the three major categories that may be used to classify distributed detection strategies. The distributed detection is discussed in further detail in the following subsections [46].

This broadcast strategy makes advantage of location information at each node, and to flood the network, they individually transmit an authorised broadcast message. Every node is answerable for storing the location data of its neighbours and eliminating any nodes that have claims that conflict with one another [38][49][56].

A node replication detection system known as Deterministic Multicast (DM) only shares a node's location assertion with a limited number of other nodes group of witness [12]. Nodes that have been picked in a deterministic manner [12][54]. In this method, each node broadcasts its claim on its location, and each of its neighbours then forwards that claim to a subset of the other nodes, which are referred to as witnesses. The number that identifies the node is used to choose the witnesses [22][44]. In the event that the attacker clones a node, then the people will get two separate position assertions from the network for the same node ID [12][13][16][36]. The DM technique is really an example that is not considered favourable (or unappealing) and is provided in; as a result, it has received only a modest amount of emphasis. On the other hand, we think it serves as an excellent illustration of the claimant–reporter–witness paradigm.

Two techniques for detecting clone attacks in wireless sensor networks, RW and table assisted RW, are discussed in the paper [15][20][25][26][27]. For every node an in the network, RW initiates many independent RWs. Once it determines which RWs each node successfully completed, it selects the nodes that passed as the witness nodes for that node. There are four stages to every RAWL run. To begin, each node sends out a signed location assertion. The second phase involves the claim being sent out probabilistically by each of the node's neighbours to a subset of nodes selected at random. In the 3rd step, selection of random nodes broadcast a message that asserts they should all begin a random stroll around the network [30] [38] [39]. The RW determines which nodes will serve as witnesses and keep the claim. In the final step, a witness may use the claims it has received to invalidate a duplicated node if it has received several claims from changed positions for the same node ID [27]. Their 2nd protocol, dubbed TRAWL, builds on RAWL by including a trace table on each and every node to reduce memory ingestion [15] [35] [39]. The RAWL method requirements extra steps to be taken at random intervals to attain a high finding possibility [35]. The resulting communication and memory overhead is more than twice as much as that of the LSM [33] [38]. The proposed TRAWL by the authors can reduce the price of memory while keeping the price of transmission constant.

## RELATED WORKS

The brief survey of different varieties of security methods under the groupings such as layered security measures, cross-layer security measures, and cryptography-based authentication and authorization methods [15][32]. After the review of these research methods, we present the research gaps of recent state-of-art methods.

### Layered Security Measures

The identification labels for SNs are generated with the help of a hash technique, and a trust evaluation model is constructed using the beta density function as its foundation.

The authors of the paper [48] offer multidimensional trust indicators that are obtained from communication between neighbouring sensor nodes.

In the article [49], the authors offer a fuzzy-based hierarchical trust management scheme. This system combines direct trust calculation based on real-time previous experience and credit-based calculation, as well as indirect trust calculation based on peer endorsement. In this particular plan, CH and BS were responsible for maintaining a constructive knowledge table that was based on fuzzy logic, which helped to decrease the amount of memory and communication overhead.

The most prevalent forms of assault were initially scrutinised. And then, under the distributed trust model, a dynamic time frame was established, which included the detection of direct trust as well as indirect trust. The Trustworthy Tree had been developed on the basis of the trusted nodes [68] [77].

In the article [99], the author suggested a trust scheme for clustered WSNs that was both lightweight and reliable. Because it eliminates feedback between nodes, it has the potential to significantly boost system

efficiency while simultaneously diminishing the impact of malicious nodes. When it comes to collaboration amongst CHs, using a dependability-enhanced trust assessing technique may successfully identify and avoid the behaviour of CHs that are malevolent, self-centred, or flawed.
In their is determined by both the direct trust and the indirect trust that it has [13] [17]. In situations in which a subject node is unable to directly see the communication behaviours of an object node, the subject node will instead acquire an indirect trust value of other nodes [7] [13] [17] [18] [26].
A trust-based intrusion detection technique was given by the author in [51] [7]. It makes use of an investigative model in addition to a statistical method for calculating the likelihood of a false alarm, and it takes into account both the trust in the quality of the service and the trust that people have in one another as trust metrics [13] [17] [7] [18] [26]. They use honesty as a measurement of social trust, as well as energy and cooperation as a measurement of the trustworthiness of service quality.
In [52-54], haves have offered several unique strategies. Intimacy, honesty, selflessness, and vitality were the four main aspects of trust that were taken into consideration.
This approach is limited to identifying a DDoS that is caused by a jamming assault [28] [53] [75].

**Cross-Layer Attack Detection Methods**

The above all are the trust-based security solutions proposed at different layers for the WSNs. However, none of the above considers the trust evaluations using the multiple layers. As was said previously, the methods that are based on a single layer are ineffective and insufficient to identify the harmful threats that are present in WSNs; hence, the cross-layer strategies that have been established in the recent past were developed.
The cross-layer method has been presented by the authors in [55] for the purpose of attack detection in MANET and WSN. They devised a method that consists of two levels of detection in order to identify malicious nodes in MANETs. At the beginning of the game, specialised sniffers operating in promiscuous mode are deployed. Every sniffer makes use of a classifier based on a decision tree, which, at each reporting time, produces a certain quantity of what are known as correctly classified instances (CCIs) [7].
For the purpose of countering cross-layer security assaults in wireless networks, a new framework known as FORMAT was presented in reference [28][29][56]. The FORMAT included of a detection component as well as a mitigation component, and it was based on Bayesian learning. On the one hand, the component responsible for attack detection builds a model out of the information that has been seen in order to identify covert attack actions. The optimization theory is used by the mitigation component in order to establish the optimal balance that is required between performance and security.
The model was built on a cross-layer technique that was described in [57] to identify sinkhole attacks in wireless sensor networks (WSNs) [14]. The author is responsible for the creation of both the detection and prevention algorithms [19] [21] [29].
The author of [58] ignored the monolithic implementation of the cross-layer method and instead used a component-based architecture [49]. An architecture that is driven by events and makes use of zero-copy buffers and metadata to address challenges that span across many domains [7].
The author developed the first properly built trust-based cross-layer attack detection framework for WSNs in [7] [17] [29]. This framework was intended to identify attacks on wireless sensor networks. They developed a trust-based intrusion detection technique for protocol layers of wireless sensor networks. The author focused primarily on considering these three facets of trustworthiness: the trustworthiness of the physical layer, the trustworthiness of the media access control layer, and the trustworthiness of the network layer. After that, the individual trust measures for each layer are added together to provide an overall trust metre for a sensor node [7] [18].
A more current proposal for a cross-layer trust-based attack detection technique may be found in reference [59]. The strategy outlined is conceptually comparable to this approach. The protocol layer trust-based IDS, also known as LB-IDS [7], is an idea that has been presented to protect the WSN by finding attackers at many levels [7]. The variation of trust metrics at each tier in relation to the assaults is used in the calculation used to determine the value of trust associated with a sensor node [13] [17]. Taking into account the most important trust metrics of a given layer allows one to determine how trustworthy a sensor node is at a certain layer. In the last step, the individual trust values of each layer are combined to arrive at an estimate of the total trust value of the sensor node [22][74]. When the trust threshold is applied, it is possible to determine whether or not a sensor node should be trusted [15] [22] [43].
The authors of [60] detect occurs between the network and MAC levels of the OSI model. XLID was validated in comparison to typical (non-cross-layered) IDS, which are based on single-layer protocols.
The author presents a strategy to limit the impact of sinkhole attacks on networks by making use of the cross-layer methods in [51] [61]. In order to improve the network's overall security, the activities that take place at

the network and MAC layers are combined [67]. The suggested research will hunt out the rogue node in the network by measuring the intensity of the signal and identifying each node.

**Authentication and Authorization Methods**

Trust-based methods can detect and prevent network attacks. Such techniques protect the network from such attacks. However, privacy preservation and data security in unreliable communication channels are still the problems for such networks [8]. This section presents the reviews of some recent works for authentication and authorization [9].

In the article [62], the authors offer a safe and by making use of the suitable intelligent e-health portals [8]. This engineering is intended to make the frameworks more productive. They deployed sensors in medical applications that were very resource demanding; as a result, they are unable to adapt to cryptographic methods that need large computations. They suggested a design that makes use of adapted intelligent e-health doors that carry out [8]. This was done in order to overcome the obstacle that had been identified [8][9].

It was suggested in [63] that MANES should use a separate tiered spine procedure. This protocol used skilled extreme discovery in order to find a method to construct clusters having hubs that are within a certain pre-specified wireless jump separation.

The authors of [64] have suggested the key management strategies for WSNs, although the authors did not identify any specific application in which these techniques would be advantageous.

The authors of [65] suggest a lightweight encryption algorithm that can be run on FPGAs for WSNs. The effectiveness of the XTEA algorithm when employed in conjunction with the confused key was analyzed and compared to the performance of other classic lightweight encryption techniques [68] [77].

The authors of [66] suggest an ECC-based encryption scheme that makes use of homomorphism encryption. The GASONeC method, which used for the encryption pattern, which had been built on it [37] [41]. ECC was formerly applied to swap open and private keys as a result of its capability to provide a high level of security while having a key size of just 176 bits [8][9].

The authors of the article [67] provided the design and implementation of a lightweight hub validation protocol, which covers hub enlistment, hub confirmation, and important foundation stages [37] [45]. However, neither a digital signature technique nor any open key cryptography is used in any way [37].

The way that the sensor hubs respond is by combining the information that is associated with many existing together questions into a single bundle, which brings about a reduction in the cost of transmission [8]. The additively homomorphic encryption is used by the hubs that act as middlemen to calculate the deciphered data [9].

The authors of the 125 documents provide a proposal for the construction and research of the authenticated key algorithm [37]. They demonstrated the improvement in performance as well as the increase of security in comparison to other methods already in use [37] [41].

A full analysis of the many different authentication mechanisms for the internet of things was published in reference [68]. In the field of Internet of Things communications employing WSNs, they examined more than forty different authentication methods and algorithms. They discussed the prospects, problems, and rewards of the situation.

Another unique routing technique for data integrity solutions that is also efficient with energy was suggested in the paper [69]. LEACH's cryptographic methods were developed specifically to solve the concerns of network security that were raised by WSNs [59].

The art and craft of a lightweight cryptographic protocol was presented in [70]. They disassemble a great deal of lightweight cryptographic methods according to the size of their keys, the size of their squares, the number of rounds, and the structures of the algorithms. In addition to this, they investigate the security engineering that is used in IoT for a required device state and concentrate on researching obstacles, concerns, and solutions.

The authors of the paper [ 70] offer a unique protocol for safe routing for WSNs with multi-variant tuples that makes use of the Two-Fish cryptography approach to identify and mitigate the effects of attackers [8] [37] [45]. They based the architecture of the model on something called the Authentication and Encryption Model (ATE Model).

Recent research published in [71] proposes an energy-efficient safe routing strategy for Internet of Things–enabled wireless sensor networks (WSNs), They devised the energy-efficient clustering process by making use of the various characteristics of the sensor nodes [8]. During the process of data transfer, they used threshold-based cryptography approaches to ensure the integrity of the sensor data as well as its security.

The authors of [72] and [73] proposed a routing strategy for WSN that ensured the safety of data transfer [8]. After that, an energy-efficient authentication system that was based on cryptography and used a progressive key-generation approach was employed.

## III. CONCLUSION

- A detailed review of experimental procedure adopted in node replication attack(NRA) mitigation investigation is presented.
- The layered trust-based mechanism for attack detection WSN failed to detect the cross-layer attacks like MIMA.
- The inability to properly optimise resources using this method in the absence of an effective clustering mechanism for WSNs is the cause of the issue. When compared to other kinds of routing algorithms, clustering has previously been shown to be a more energy-efficient option for resource-limited WSNs. Provide cross-layer solutions that are not vulnerable to the numerous issues provided by WSNs, such as the maintenance of data security and privacy.
- The goal of the research into cryptography-based solutions was to provide privacy preservation in wireless sensor networks (WSNs). But these solutions aren't without their problems, such the fact that some of them simply concentrate on privacy protection and don't bother with clustering at all. A few of the approaches did not take into account the trustworthy relay selection required for safe data transfers.

The NRA has hazardous impacts on WSN and its security goals. This research deals with various existing detection, prevention and recovery approaches for NRA. Also, this classifies and compares merits and demerits of various existing protocols for mitigation. In both WSN and MWSN, there was a proposal made to create a taxonomy of centralised and distributed methods for finding NRAs [15][20][25]. Existing distributed witness node-based detection schemes of NRA are vulnerable to attacks known as smart attack of which are variations of NRA [25]. These attacks are a source of vulnerability for these detection schemes [20]. In the next chapters, unique solutions to some of the problems inherent in the already implemented strategies will be proposed [8]. We have studied the various research works for security in IoT enabled applications using WSNs in this chapter. According to the functionality of these methods, we have defined the research gaps as a motivation of the proposed models [9][22][41].

## REFERENCES


1. Kore, A., Patil, S. IC-MADS: IoT Enabled Cross Layer Man-in-Middle Attack Detection System for Smart Healthcare Application. Wireless Pers Commun 113, 727–746 (2020). https://doi.org/10.1007/s11277-020-07250-0.
2. Gilbert, E. P. K., Baskaran, K., Rajsingh, E. B., Lydia, M., & Selvakumar, A. I. (2019). Trust aware nature inspired optimised routing in clustered wireless sensor networks. International Journal of Bio-Inspired Computation, 14(2), 103. doi:10.1504/ijbic.2019.101637.
3. Haseeb, K., Islam, N., Almogren, A., Din, I. U., Almajed, H. N., & Guizani, N. (2019). Secret Sharing-based Energy-aware and Multi-hop Routing Protocol for IoT based WSNs. IEEE Access, 1–1. doi:10.1109/access.2019.2922971.
4. Alghamdi, T. A. (2018). Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method. IEEE Access, 1–1. doi:10.1109/access.2018.2865909.
5. Kanoosh, Huthaifa & Houssein, Essam & Selim, Mazen. (2019). Salp Swarm Algorithm for Node Localization in Wireless Sensor Networks. Journal of Computer Networks and Communications. 2019. 1-12. 10.1155/2019/1028723.
6. Sharma, R., Vashisht, V., & Singh, U. (2020). eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks. Telecommunication Systems. doi:10.1007/s11235-020-00654-0.
7. Rodrigues, P., John, J. Joint trust: an approach for trust-aware routing in WSN. Wireless Netw (2020). https://doi.org/10.1007/s11276-020-02271-w.
8. Ramesh, S., & Yaashuwanth, C. (2019). Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. Multimedia Tools and Applications. doi:10.1007/s11042-019-7585-5.
9. Mabodi, K., Yusefi, M., Zandiyan, S. et al. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. J Supercomput 76, 7081–7106 (2020). https://doi.org/10.1007/s11227-019-03137-5.
10. Agarwal, M, Biswas, S & Nandi, S 2015, 'Detection of De-Authentication DoS Attacks in Wi-Fi Networks: A Machine Learning Approach,' in Proc. of IEEE International Conference on Systems, Man, and Cybernetics, pp. 246 – 251

11. Agarwal, M, Purwar, S, Biswa, S & Nandi, S 2017, 'Intrusion detection system for PS-Poll DoS attack in 802.11 networks using real time discrete event system,' in IEEE/CAA Journal of Automatica Sinica, vol. 4, no. 4, pp. 792-808.
12. Alazab, A, Hobbs, M, Abawajy, J & Khraisat, A 2013, 'Malware Detection and Prevention System Based on Multi-Stage Rules', International Journal of Information Security and Privacy (IJISP), vol. 7, no. 2, pp. 29-43.
13. Alazab, M, & Batten, LM 2015, 'Survey in Smartphone Malware Analysis Techniques. In M. Dawson, & M. Omar (Eds.)', New Threats and Countermeasures in Digital Crime and Cyber Terrorism, Hershey, PA: IGI Global, pp. 105-130.
14. Aminanto, ME, Choi, R, Tanuwidjaja, HC, Yoo, PD & Kim, K 2018, 'Deep Abstraction and Weighted Feature Selection for Wi-Fi Impersonation Detection,' in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 621-636.
15. Banescu, S, Wuchner, T, Salem, A, Guggenmos, M, Ochoa, M & Pretschner, A 2015, 'A framework for empirical evaluation of malware detection resilience against behavior obfuscation,' 10thInternational Conference on Malicious and Unwanted Software (MALWARE), Fajardo, pp. 40-47.
16. Bernhard Seeger, 'DYNAMIC Not Only has the Engine mattered! Complex Event Processing', Available online: https://db.in.tum.de/hosted/scalableanalytics/presentations/CEP_Dyna mic. pdf, as on 10.11.2017
17. Beuhring, A & Salous, K 2014, 'Beyond Blacklisting: Cyberdefense in the Era of APTs,' in IEEE Security & Privacy, vol. 12, no. 5, pp.90-93.
18. Beyah, R & Venkataraman, A 2011, 'Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions,' IEEE Security & Privacy Magazine, vol. 9, no. 5, pp. 56–61.
19. Boris Lau & Sophos Plc 2008, 'Dealing with Virtualization packers -CARO Workshop 2008', (n.d.). Available online : http://2008.caro.org/program/dealing-with-virtualization-packers.
20. Brookes, S, Osterloh, M, Denz, R & Taylor, S 2015, 'The KPLT: The Kernel as a shared object,' Military Communications Conference, MILCOM IEEE, Tampa, FL, pp. 954-959.
21. Buhov, D, Huber, M, Merzdovnik, D & Weippl, EV2016, 'Pin it! Improving Android network security at runtime', IFIP Networking Conference (IFIP Networking) and Workshops, Vienna, pp. 297-305.
22. Cabaj, K & Mazurczyk, W 2016, 'Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall,' in IEEE Network, vol. 30, no. 6, pp. 14-20
23. Chamotra, S, Bhatia, JS, Kamal, R & Ramani, AK 2011, 'Deployment of a low interaction honeypot in an organizational private network,' International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Udaipur, pp. 130-135.
24. He, Tian, Sudha Krishnamurthy, John A. Stankovic, Tarek Abdelzaher, Liqian Luo, Radu Stoleru, Ting Yan, Lin Gu, Jonathan Hui, & Bruce Krogh. "Energy-efficient surveillance system using wireless sensor networks." In Proceedings of the 2nd international conference on Mobile systems, applications, & services, pp. 270–283. ACM, 2004.
25. Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, & Erdal Cayirci. "Wireless sensor networks: a survey." Computer networks 38, no. 4 (2002): 393–422.
26. Nadeem, Adnan, Muhammad Azhar Hussain, Obaidullah Owais, Abdul Salam, Sarwat Iqbal, & Kamran Ahsan. "Application specific study, analysis & classification of body area wireless sensor network applications." Computer Networks vol. 83, pp. 363–380.2015.
27. The Mobile Economy, GSMA, 2013.
28. Kirby, Karen K. "Hours per patient day: not the problem, nor the solution."Nursing Economics 33, no. 1 (2015): 64.
29. Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. SN Appl. Sci. 3, 121 (2021). https://doi.org/10.1007/s42452-021-04156-9.
30. Bhushan B., Sahoo G. (2020) Requirements, Protocols, and Security Challenges in Wireless Sensor Networks: An Industrial Perspective. In: Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security. Springer, Cham. https://doi.org/10.1007/978-3-030-22277-2_27.
31. Xiaoxia Huang, Hongqiang Zhai, and Yuguang Fang, "Robust Cooperative Routing Protocol in Mobile Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Vol. 7, No..12, 2008, pp. 5278-5285.
32. David Braginsky and Deborah Estrin, "Rumor Routing Algorthim For Sensor Networks." in 1st ACM international workshop on Wireless sensor networks and applications,2002,pp. 22-31.
33. Elahmadi Cheikh, Chakkor Saad,Baghori Moustafa, Hajraoui Abderrahmane, "A New Approach to Improving Lifetime in Heterogeneous Wireless Sensor Networks Based on Clustering Energy Efficiency

Algorithm", Journal of Theoretical and Applied Information Technology, Vol. 61, No. 2, March 2014,pp. 405-412.
34. S. Lindsey and C. Raghavendra. "PEGASIS: Power-Efficient Gathering in Sensor Information Systems". In IEEE Aerospace Conference 2002, Vol. 3, pp. 1125-1130.
35. A.V.Sutagundar and S. S. Manvi. "Location Aware Event Driven Multipath Routing in Wireless Sensor Networks: Agent Based Approach", Egyptan Informatics Journal, Vol.14, No.1,2013, pp. 55-65.
36. Kee-Young Shin, Junkeun Song, JinWon Kim, Misun Yu, and Pyeong Soo Mah., " REAR: Reliable Energy Aware Routing Protocol for Wireless Sensor Networks", in 9th IEEE International Conference on Advanced Communication Technology, Vol. 1,2007, pp. 525-530.
37. Ghassan Beydoun, Graham Low, and Paul Bogg, " Suitability Assessment Framework of Agent-Based Software Architectures",Journal of Information and Software Technology, Elseiver,Vol.55, No.4, 2013, pp. 673-689.
38. Kim, M., S. Kim, J. Seo, K. Choi and S. Han (2014). CAPNet: An Enhanced Load Balancing Clustering Algorithm for Prolonging Network Lifetime in WSNs International Journal of Distributed Sensor Networks, Vol. 2014, Art. ID 234394, pp. 1-8.
39. Yu, T., S. Liu and Z. Zhang (2015). A Cluster-based Uneven Grid Data Aggregation in Wireless Sensor Networks, Journal of Computational Information Systems, Vol. 11, No. 19, pp. 7055-7062.
40. Nam, C.S., Y.S. Han and D.R. Shin (2013). The Cluster-Heads Selection Method considering Energy Balancing for Wireless Sensor Networks, International Journal of Distributed Sensor Networks, Vol. 2013, Article ID 269215, pp. 1-6.
41. Yuan, F., Y. Zhan and Y. Wang (2014). Data Density Correlation Degree Clustering Method for Data Aggregation in WSN, IEEE Sensors Journal, Vol. 14, No. 4, pp. 1089-1098.
42. Sabet, M. and H.R. Naji (2015). A decentralized energy efficient hierarchical cluster based routing algorithm for wireless sensor networks, International Journal of Electronics and Communications, Vol. 69, No. 5, pp. 790-799.
43. Shankar, T. and S. Shanmugavel (2014). Energy Optimization in Cluster Based Wireless Sensor Networks, Journal of Engineering Science and Technology, Vol. 9, No. 2, pp. 246-260.
44. Tang, C., S.K. Shokla, G. Modhawar and Q. Wang (2016). An Effective Collaborative Mobile Weighted Clustering Schemes for Energy Balancing in Wireless Sensor Networks, Sensors, Vol. 16, No. 2, pp. 1-19.
45. A. J. Joseph and U. Hari, "Hexagonally sectored routing protocol for wireless sensor networks," Int. J. Eng., vol. 2, no. 5, pp. 1249–1252, May 2013.
46. Qi-Ye Zhang, Ze-Ming Sun, Feng Zhang, "A Clustering Routing Protocol for Wireless Sensor Networks Based on Type-2 Fuzzy Logic and ACO", 2014 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE) July 6-11, 2014, Beijing, China
47. Muhammad Amjad ; Muhammad Khalil Afzal ; Tariq Umer ; Byung-Seo Kim, "QoS-Aware and Heterogeneously Clustered Routing Protocol for Wireless Sensor Networks", IEEE Access ( Volume: 5 ), 2017
48. Peyman Neamatollahi, Mahmoud Naghibzadeh, Saeid Abrishami, Mohammad-Hossein Yaghmaee,"Distributed Clustering-Task Scheduling for Wireless Sensor Networks Using Dynamic Hyper Round Policy", IEEE TRANSACTIONS ON MOBILE COMPUTING, TMC-2016-02-0080, 2017
49. Han, G., Zhou, L., Wang, H., Zhang, W. and Chan, S. (2017), 'A source location protec- tion protocol based on dynamic routing in wsns for the social internet of things', Future Generation Computer Systems 82(1), 689–697.
50. Lee, I.-G. and Kim, M. (2016), 'Interference-aware self-optimizing wi-fi for high effi- ciency internet of things in dense networks', Computer Communications 89(1), 60–74.
51. Mahajan, S., Malhotra, J. and Sharma, S. (2014), 'An energy balanced qos based cluster head selection strategy for wsn', Egyptian Informatics Journal 15(3), 189–199.
52. Khan, B. M., Bilal, R. and Young, R. (2017), 'Fuzzy-topsis based cluster head selection in mobile wireless sensor networks', Journal of Electrical Systems and Information Technology 4(3), 89–101.
53. Wang, W., Hu, L. and Li, Y. (2010), 'Security analysis of a dynamic program update protocol for wireless sensor networks', IEEE Communications Letters 14(8), 782–784.
54. Ke, W., Yangrui, O., Hong, J., Heli, Z. and Xi, L. (2016), 'Energy aware hierarchical cluster-based routing protocol for wsns', The Journal of China Universities of Posts and Telecommunications 23(4), 46–52.
55. Kannan, G. and Raja, T. S. R. (2015), 'Energy efficient distributed cluster head schedul- ing scheme for two tiered wireless sensor network', Egyptian Informatics Journal 16(2), 167–174.
56. Shankar, T., Shanmugavel, S. and Rajesh, A. (2016), 'Hybrid hsa and pso algorithm for energy efficient cluster head selection in wireless sensor networks', Swarm and Evolutionary Computation 30(1), 1–10.

57. Song, L., Chai, K. K., Chen, Y., Schormans, J., Loo, J. and Vinel, A. (2017), 'Qos- aware energy-efficient cooperative scheme for cluster-based iot systems', IEEE Systems Journal 11(3), 1447–1455.
58. Sirdeshpande, N. and Udupi, V. (2017), 'Fractional lion optimization for cluster head- based routing protocol in wireless sensor network', Journal of the Franklin Institute 354(11), 4457–4480.
59. Sharma, R., Vashisht, V., & Singh, U. (2019). Nature Inspired Algorithms for Energy Efficient Clustering in Wireless Sensor Networks. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). doi:10.1109/confluence.2019.8776618.
60. Sharma, R., Vashisht, V., & Singh, U. (2019). EEFCM-DE: Energy Efficient Clustering Based on Fuzzy C Means and Differential Evolution Algorithm in Wireless Sensor Networks. IET Communications. doi:10.1049/iet-com.2018.5546.
61. Pavani, M., & Trinatha Rao, P. (2019). Adaptive PSO with Optimized Firefly Algorithms for Secure Cluster Based Routing in Wireless Sensor Networks. IET Wireless Sensor Systems. doi:10.1049/iet-wss.2018.5227.
62. Gilbert, E. P. K., Baskaran, K., Rajsingh, E. B., Lydia, M., & Selvakumar, A. I. (2019). Trust aware nature inspired optimised routing in clustered wireless sensor networks. International Journal of Bio-Inspired Computation, 14(2), 103. doi:10.1504/ijbic.2019.101637.
63. Ramesh, S., & Yaashuwanth, C. (2019). Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. Multimedia Tools and Applications. doi:10.1007/s11042-019-7585-5.
64. Sharma, R., Vashisht, V., & Singh, U. (2020). eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks. Telecommunication Systems. doi:10.1007/s11235-020-00654-0.
65. Mahajan, H.B., Badarla, A. Cross-Layer Protocol for WSN-Assisted IoT Smart Farming Applications Using Nature Inspired Algorithm. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-08866-6.
66. Shao, N.; Zhou, Z.; Sun, Z. A Lightweight and Dependable Trust Model for Clustered Wireless Sensor Networks. In Proceedings of the International Conference on Cloud Computing and Security, Nanjing, China, 13–15 August 2015; pp. 157–168.
67. Luo, W.; Ma, W.; Gao, Q. A dynamic trust management system for wireless sensor networks. Sec. Commun. Netw. 2016, 9, 613–621.
68. Hu, Zhi & Bie, Yuxia & Zhao, Hong. (2015). Trusted Tree-Based Trust Management Scheme for Secure Routing in Wireless Sensor Networks. International Journal of Distributed Sensor Networks. 2015. 1-13. 10.1155/2015/385849.
69. Li, X.; Zhou, F.; Du, J. A lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans. Inf. Forensics Secur. 2013, 8, 924–935.
70. Jiang, J.; Han, G.; Wang, F.; Shu, L.; Guizani, M. An efficient distributed trust model for wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. 2015, 26, 1228–1237.
71. M. M. Ozcelik, E. Irmak and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," 2017 International Symposium on Networks, Computers and Communications (ISNCC), 2017, pp. 1-6, doi: 10.1109/ISNCC.2017.8071998.
72. Wang, N., Wang, J., & Chen, X. (2019). A Trust-Based Formal Model for Fault Detection in Wireless Sensor Networks. Sensors (Basel, Switzerland), 19(8), 1916. https://doi.org/10.3390/s19081916.
73. Zhang, T.; Yan, L.; Yang, Y. Trust evaluation method for clustered wireless sensor networks based on cloud model. Wirel. Netw. 2016.
74. P. T. Sharavanan & D. Sridharan, & R. Kumar, "A Privacy Preservation Secure Cross Layer Protocol Design for IoT Based Wireless Body Area Networks Using ECDSA Framework," Journal of Medical Systems (2018) 42:196.
75. Rajeswari, S. R., & Seenivasagam, V. (2016). Comparative Study on Various Authentication Protocols in Wireless Sensor Networks. The Scientific World Journal, 2016, 1–16. doi:10.1155/2016/6854303.
76. Alhayani, B., Abbas, S.T., Mohammed, H.J., & Mahajan, H. B. Intelligent Secured Two-Way Image Transmission Using Corvus Corone Module over WSN. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-08484-2.
77. Wang Wei-hong, Lin Yu-bing& Chen Tie-ming 2008, 'The Study andApplication of Elliptic Curve Cryptography Library on WirelessSensor Network', 11th IEEE Conference on Communication Technology Proceedings. Hangzhou, pp. 785-788.