JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

Security Assaults, Its Counter Measures and Difficulties over a Sensor Cloud

[1]Vijayasanthi Maddela,

Assistant Professor, Department of C.S.E, Sree Vidyanikethan Engineering College, Tirupati, India.

[2]Ashok Patel,

Assistant Professor, Department of CS, Florida Polytechnic University, IST 2068,
4700, Research Way, Lakeland, FL 33805-8531.USA.

[3]K. Rangaswamy,

Assistant Professor, Department of C.S.E, Sai Rajeswari Institute of Technology, Proddatur, India.

[4,*]K. Reddy Madhavi,

Professor, Department of C.S.E, Sree Vidyanikethan Engineering College, Tirupati, India.

[1]vsmaddelasanthi@gmail.com
[2]apatel@floridapoly.edu
[3]rangaswamy19@gmail.com
[4]kreddymadhavi@gmail.com
Corresponding Author: K. Reddy Madhavi

Abstract

Sensor hubs in a Wireless Sensor Network include sound sensors, camera sensors, temperature sensors, proximity sensors, movement sensors, light sensors, shade sensors, and accelerometer sensors. Sensor hubs have several limitations, including restricted memory, power, and handling. W.S.N.'s capabilities have expanded significantly in recent years and include social insurance monitoring, disaster detection, military applications, savvy home inspection, and alert urban communities, among other things. Despite its various applications, adaptability, hub control, asset booking, board portability, and security are some of the research difficulties with W.S.N. Increasing the number of sent sensors to fulfil demand is difficult with the growing popularity of W.S.N. applications. In this approach, cloud and virtualization can help with the problem. Sensor Cloud is the result of combining cloud and W.S.N. One of the research issues that sensor clouds encounter is security. This study, reported in this publication, focuses on a few of the most severe security breaches in sensor clouds.

Keywords: *Security Threats, Sensor Clouds, Wireless Sensor Networks, Cloud Computing, and Challenges*.

1. Introduction

In the sensor cloud, W.S.N. and cloud are reconciled. Thanks to distributed computing features, it provides a platform for scalability and data management. The benefits of distributed computing are numerous, including enormous storage and computational capabilities, data security, continuous data processing, adaptability, multi-tenancy, and so on, all of which outweigh the drawbacks of W.S.N. Sensor clouds send data from sensor hubs to the cloud for processing, allowing us to access data in a fraction of a second from any location and at any time. Customers are encouraged to seek, prepare, perceive, deconstruct, save, and share knowledge. The remainder of the paper is sorted into pursues. In region II,

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

favourable sensor cloud conditions are discussed. Area III exhibits sensor cloud applications, whereas segment IV focuses on sensor cloud attacks. Area V introduces writing reviews, and segment VI wraps up a piece of paper with possible future headings.

2. Advantages of the sensor cloud

Sensor to cloud reconciliation has a few advantages. The following are some of them:

The Sensor- Cloud boosts the necessity to cope with the adjustable sensor arrangement when the system size grows swiftly.

Increases are accumulating power- The sensor data is large in size because the sensors gather it for observing/dissecting.

Distributed storage is the primary instrument for storing such a large amount of data.

3. Sensor Cloud Applications

Sensor clouds are being employed in a wide range of applications right now. They boosted handling capacity—Cloud offers a wide range of helpful data preparation and analysis capabilities. Because it provides an easy stage for the end-user to conduct a range of activities on the data, tools like Math Engine [30] allow one to break down, process, and screen data in various critical ways.

Administrations' accessibility Because of the universal access property of the cloud, it is simple to access administrations from anywhere and at any time.

Multi-tenancy is the sharing of a program's event among a large number of customers, such as when a single programme is used to meet the needs of a large number of clients simultaneously.

Resource advancement and asset utilization Sensor-Cloud allows you to improve and use your assets better. Advancement is achieved by resource sharing and the selective use of the most critical resources. They are divided into two categories as follows:

A. Cloud-based sensor applications that are already in use:
- Microsoft HealthVault
- Pachube
- ThingSpeak
- Nimbits
- iDigi

B. Sensor-Cloud is being used in a variety of new ways:
- Health-monitoring software (utilizing wearable sensors, for example, Fit bit and so forth.)
- Detection and monitoring of disasters (for example, seismic tremors, floods and so forth.)
- Unmanned Aerial Vehicles (UAVs)
- IoT

4. Sensor Research Methodology

The authors in [5] Provide the approach for conducting a deliberate writing audit (S.L.R.). The fundamental purpose of directing S.L.R. is to carry out a well-organized writing study to address the Research Questions posed during the investigation's preliminary stages. S.L.R. enables experts to locate, evaluate, and combine the exploration factors led by several system security experts

The following steps are involved in enhancing S.L.R.:

Development of a complete method to leading S.L.R. of security attacks utilizing machine and deep learning applications

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

as part of an audit.

• Enumerate the Research Questions regarding security assaults using the PICO search process [6].

• To react to the exploration questions and synthesize the selected examinations.

QUESTIONS FOR RESEARCH

Characterizing Research Questions (R.Q.s) is the most significant advancement in the orderly audit. The examination's R.Q.'s keep the flow going at first. This article uses a PICO system to characterize R.Q.s, which comprises many sections describing the study's nature. The following are the issues that the investigation focuses on when it comes to an attack on security in a remote sensor cloud:

• RQ1. What are the many forms of dynamic assau that could be a major problem in the context distributed systems?
• RQ2. What are the numerous options known approaches for dealing with latent assaults?
• RQ3. What are the various arrangements that ar used?
• RQ4. How are countermeasures devised for a variety of attack techniques that have an impact on the examination?

SEARCH METHODS

The efficient investigation aims to use an orderly methodology to locate, consider, and characterize present research ponders within the class irregularity concerns. For the searching technique, well-known logical databases such as IEEE, SPRINGER, A.C.M., SCIENCE DIRECT, and Google researcher libraries are used, with the accompanying pursuit strings in various blends.

In the underlying causes, we identified roughly 217 research articles concerning the class unbalanced concerns distributed in the past decade throughout the examination using the search above keyword. Table 1 depicts many web components that can be utilized to search for relevant examinations

---

Attacks and Countermeasures in the Cloud on Active Wireless Sensor Networks

OR

In the Cloud, Passive Wireless Sensor Network Attacks and Countermeasures

AND

The Challenges of Secure Sensor-Cloud Computing

AND

Security Attacks on Wireless Sensor Networks and Countermeasures

AND

A Systematic Study of Security in the Sensor-Cloud

OR

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

Sensor cloud issue

Table 1: Different Scientific databases considered for S.L.R.

S.No	Database	Number of Papers
1	IEEE	110
2	SPRINGER	10
3	ACM	52
4	GOOGLE SCHOLAR	20
5	SCIENCE DIRECT	25
Total		217

Productions Related to the sorts of security assaults

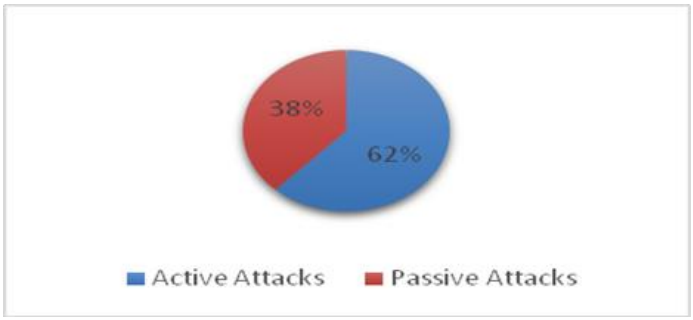

Figure 1: Quantitative analysis of distributions Associated with various types of security attacks

Selection of preliminary articles

Three hundred related papers are retrieved from scientific databases using search strings in the preliminary phase of the selection, and articles are appraised based on the title's relation to the issue statement, with the other articles being ignored. Furthermore, the study does not include articles from theses, book chapters, short papers, and publications written in languages other than English. The abstract, title, and conclusion of the paper publications are used to determine whether or not they should be included in the study. As a result, the relevant articles are filtered according to their relevance to the topic of class imbalance.

Title: (Active assaults, passive attacks, centric tactics, application-layer attacks, network attacks, network traffic, software-defined networking, and cloud computing are examples of active attacks, passive attacks, and centric techniques.)

AND

Abstract: (Security mechanisms, network security strategies and approaches, countermeasures, and cloud security issues are all examples of security mechanisms.)

The articles were chosen based on the details of the implementation and the data sets that were used.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

We further break down the nature of articles based on the intricacies of usage provided in the article at this level, to the point where the item is thoroughly analyzed.

The survey process considers the computation utilized to determine security assaults in arrangements and their implementation with real-world datasets. Furthermore, papers that provide a detailed description of the calculation rely on the procedure's curiosity. In light of the suppositions and proposals of the specialists with involvement in the way toward directing a deliberate survey in different spaces, search strings are altered to be progressively focused on the subject and previously outfitted. The S.L.R. technique is thought to improve due to criticism from a group of research professionals. Part 5 is devoted to a detailed examination of various systems and techniques. To security, assaults are provided. Table 2 shows the criteria for consideration and rejection for the investigation choice. Finally, based on the consideration and rejection criteria, 34 items are considered for the survey, all of which have security assaults and issues.

Table 2: Criteria for Inclusion and Exclusion

Inclusion Criteria	**Exclusion Criteria**
Security systems relating to the difficulties are discussed in articles.	Articles that are ambiguous in their application of the suggested instruments
Articles arranged according to evidence-based research on security attacks, with a fair depiction of usage intricacies that includes datasets, instruments, and systems	Regarding the security assaults, white papers and lecture notes are available.
Articles that are essentially current in the field of software engineering	Other than English, articles are written in a variety of languages.
Articles written in English are known as English-language articles.	

5. Security attacks classification and Prevention measures

The need to ensure the security of sensor data intended for cloud storage derives from the widespread reliance on cloud storage of data, as well as several security vulnerabilities. Sensor-Cloud Assaults can happen on either the sensor (W.S.N.) or the cloud.

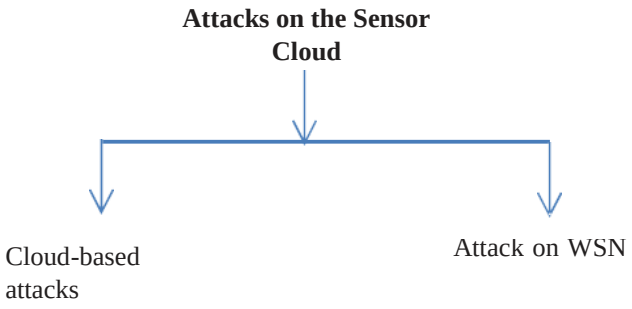

Figure.2: Sensor-Cloud attacks.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

Attacks on Cloud

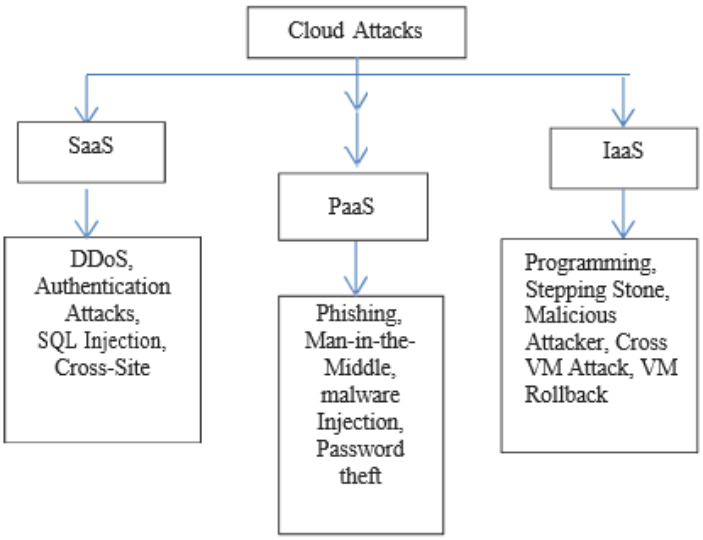

Figure.3: Cloud Attacks.

Attacks on W.S.N.

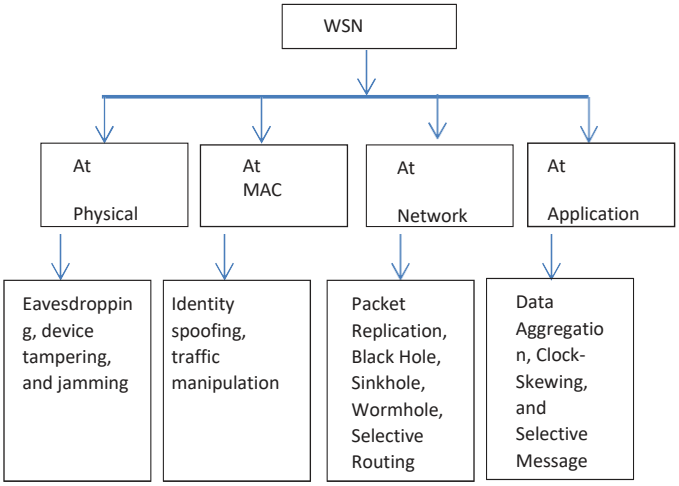

Figure.4: W.S.N. Attacks.

Table 3: Layer-based Attacks and their Counter Measures

Layer	***Attacks***	***Countermeasure***
Physical Layer	Sticking Hub Tampering Silently Listening	Access Control and Encryption
Data Link Layer	Personality Spoofing through Traffic Manipulation	Character Protection and Detection of Bad Behavior

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

Network Layer	Scrutinize data on steering Assault by Sybil Wormhole Dark Hole satirizes Hi flood Affirmation Replication of a Fake Routing Bundle	Restriction on Routing Access Detection of False Routing Information Detection of Wormholes
Transport Layer	De-synchronization due to flooding	Connection Numbers Restrictions Confirmation
Application Layer	Attacks via nefarious code Denial of Service Attacks Skewing of the Clock Message Specific Information Aggregation Distortion in Forwarding	Information Integrity and Confidentiality are both safeguarded.

6. Analysis and Quality Assessment of the Review –W.S.N. Attacks a sensor cloud

One of the significant challenges with sensor cloud is security. Despite some progress and study in the domain of sensor-cloud security, there is still a need to focus on this area. The end clients require a high level of trustworthiness and precision in the information obtained by the sensors. Therefore the information is quite valuable to them—the programmer's alteration. The proper investigation of data will not result from the collection of data. Sensor-cloud attacks can happen at the cloud, organization, or both levels.

To check protection against clock slant replication assault, Saputra et al. [19] introduced a sifting component. The undesired hops in fake timestamps are identified using this method. By supplying different timestamp values, this attack can be identified. This investigation employs a technique to distinguish between authentic and fake clock values.

A new clock-slant estimate model was presented by Zander et al. [20]. The analysis demonstrates that the suggested computation is correct and outperforms previous calculations that relied on an ad hoc scrutinizing approach.

By inventing a technique that uses higher accuracy time stamps, Jana et al. [21] stated that clock slants can be utilized to identify unapproved distant paths. Compared to other methods, such as those relying on TCP/ICMP, the designers stated that this system of slant detection is faster and requires fewer parcels.

Yu et al. [22] proposed a method for identifying specific sending assaults and distinguishing the hubs involved in the attack in W.S.N., allowing both base and source stations to identify the assault. The idea behind the offered multi-bounce affirmation scheme is that the moment a hub in the network detects hostile behaviour from other hubs (following this specific hub), an admonition bundle will be sent to the base station.

Kaplantzis et al. [23] advocated using help vector machines at the base station to locate specific transmitting assaults in W.S.N. The Intrusion Detection System uses data directed by the base station to generate cautions based on transfer speed and jump check. This may accurately identify assaults such as dark gap assaults and specific sending assaults.

In the W.S.N., Wazid et al. [24] presented group-based blackhole assault detection. This methodology frames a set of hubs in which the facilitator is chosen based on reasonableness and effectiveness criteria. Furthermore, this chosen organizer will be responsible for the system's blackhole finding.

Sharmila et al. [26] advocated using Message Digest Algorithms to detect sinkhole attacks in W.S.N. The convention employs single-direction hash chains to find careful sink gaps in the system. When the condensation is sent in the trustworthy course and the new course differs, the sinkhole assault is identified using this discovery plot.

Guo et al. [27] proposed a defence against W.S.N.'s wormhole assault. The instrument used to resist such attacks is based

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

on neighbour hub confirmation, which states that when a hub accepts a control parcel, it checks to see if it came from one of its neighbours and predicts wormhole attacks.

Wormhole-versatile Geographic Distributed Localization is a limitation-based Xu et al. [28] proposed a calculation. (WGDL). The multidimensional scaling is used in this WGDL calculation (M.D.S.) technique, which freezes the entire region impacted by wormholes and can thus effectively monitor, protect, and recover from such an attack.

Chen et al. [29] offered ways to detect mocking assaults in the same way Sybil assaults are identified. The detection of both types of assaults is accomplished using the same method. Furthermore, a group-based attack indicator is developed for recognizing both assaults.

Table 4: Systems utilized to safeguard against W.S.N. assaults

Authors	***Proposed Approach***	***Remarks***
Saputra et al. [19]	Sifting	Protect yourself from a replication attack. The Clock Is Wrong.
Zander et al. [20]	Examining in real-time	Through an estimated approach for discovering shrouded administrations, a barrier against Clock-slant assault is created.
Jana [21] et al.	Least-square fit and direct programming	Defending against a clock incline attack by identifying unauthorized remote access centres
Yu et al. [22]	Affirmation System with Multiple Jumps	Provides identification by launching selective attacks.
Kaplantzis et al. [23]	Vector of Bolster Machines	Protect yourself from a Selective Forward Assault using an interruption detection system based on Support Vector Machines (SVMs) and sliding windows.
Wazid et al. [24]	A methodology based on a slew of development	Defend yourself from a black hole attack.
Gao [25] et al.	AODV Protocol Routing	Detection and defense against black hole attacks.
Sharmila et al. [26]	Algorithms for Message Digest	Protect against sinkhole attacks by calculating message digests that meet security objectives such as information uprightness, information validity, information accessibility, secrecy, and temporal synchronization.
Guo [27] et al.	Verification of Neighbor Hubs	Resistance to wormhole attacks.
Xu et al [28]	Calculations for range-free anchor-free confinement (R.F. A.F.).	Resistance to wormhole attacks
Chen[29] et al.	K-implies calculation	Defence against Identity-Based Assaults, for example, ridiculing and Sybil

7. Difficulties in Secure Sensor Cloud

The growth of sensor-distributed computing creates a massive window of opportunity for missteps and attacks. This demonstrates the need for sensor-distributed computing security, as the system's properties make it easier to manipulate, endangering the public's potential advantages. The overall purpose of this article is to look at the security threats and challenges in the sensor cloud environment, as well as to address key research areas for evaluating developing sensor-mists against various attacks. The most important study was divided into three bearings, as indicated below.

Secure Pre-organization

This course includes an examination of security considerations before the transmission of sensor data to the cloud. Sensor clouds' design must comprehend the framework's relationships, security mechanisms, attacks, and preventative measures. In this case, an examination of the universe of feasible outcomes following a successful assault can be used to determine

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 1633-1643
https://publishoa.com
ISSN: 1309-3452

whether the framework should be enhanced and, if so, in what distinct part (or crosswise over segments) to electively build the security of the complete framework.

Secure Pre-preparing

The investigation of security issues before the execution of missions is covered in this section. Before execution, we must confirm that the sensor cloud incorporates all necessary safety measures to preserve the most significant level of security. The predicate encryption was detected in this direction. Plot to be very appealing in managing confirmation and approval, and k-obscurity on multi-social informational collecting to be a developing investigation.

Secure Runtime

This topic covers the investigation of concerns discovered during the runtime of sensor-cloud security. We've found requests for secure data collecting and two-layer key administration architectures, in particular

8. Conclusion and Future work

Security will be the test, given the increasing rise of sensor cloud applications. The security of sensor data is critical, and it should never be jeopardized. Sensor cloud applications are susceptible to a wide range of threats. These assaults might happen on the cloud or the local network—the organization level. As a result, security must be implemented at both the cloud and system levels. This document demonstrates a few of the significant sensor cloud assaults and the barrier component for each, using diverse designers' experiences. The Sensor-cloud management uses three metrics to detect more recent threats and attacks: Secure Pre-Deployment to uncover structure issues, tighten arrangements, and characterize security instruments before they are deployed; Secure Pre-Processing is required to ensure that all health policies are implemented., as well as Identity, Access Management, are in place, as well as Information Privacy; Secure Post-Deployment to guarantee that all security controls have been implemented; Secure Post-Deployment to guarantee that all security controls have been implemented; Secure Post-Deployment to ensure that all security controls have been implemented in place; Secure Run-time for cloud-based sensor systems to ensure trusted sensor organize activity and essential administration approaches. For each measurement, we consider various options, combining ideas from Attack Graphs, Policy Management, Anonymization, Statistical Estimation, and Topology-aware key management. A secure system is essential for the future, and it must be simplified, engaging, and effective

References

[1] S. Garg and H. Saran, "Anti-DDoS Virtualized Operating System". Third International Conference on Availability, Reliability and Security, (pp. 667-674), 2008.

[2] Q. Chen, W. Lin, W. Dou, and S. Yu, "Cbf: A packet filtering method for ddos attack defense in cloud environment", Ninth International Conference on, 2011, pp. 427–434.

[3] L. Yang, T . Zhang, J. Song, J. Wang, and P. Chen, "Defense of ddos attack for cloud computing". International Conference on Computer Science and Automation Engineering (CSAE), volume 2,pages 626–629, 2012.

[4] D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side channels in cloud services: Deduplication in cloud storage", Security and Privacy, pp. 40 -47, 2010.

[5] Y. Sun and D. He, "Model Checking for the Defense against Cross-Site Scripting Attacks". International Conference on Computer Science and Service System, pp.1-8, 2012.

[6] A. Saxena, S. Sengupta, P. Duraisamy, V. Kaulgud and A. Chakraborty, "Detecting SQL injection vulnerabilities in Sales Force applications ", Proceeding of the International Conf on Advances in Computing, Communications and Informatics (ICACCI)., Mysore, K.A., 2013, pp. 489-493.

[7] T. Karnwal., S. Thandapanii, and A. Gnanasekaran, "A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack", Intelligent Informatics. Springer. p. 459-469, 2013.

[8] T. Li, F. Han, S. Ding, and Z. Chen, "Larx: large-scale anti- phishing by retrospective data-exploring based on a cloud computing platform", International Conference on Computer Communications and Networks (ICCCN), pp. 1–5, 2011.

[9] E. Ferguson, J. Weber, and R. Hasan, "Cloud based content fetching: Using cloud infrastructure to obfuscate phishing scam analysis", Eighth World Congress on Services, pp. 255–261, 2012.

[10] F. Zhang, Y. Huang, H. Wang, H. Chen, and B. Zang, "Palm:Security preserving vm live migration for systems with vmm-enforced protection", Trusted Infrastructure Technologies Conference, 2008. APTC '08. Third Asia-Pacific, oct. 2008, pp. 9 – 18.

[11] Z. Chen, F. Han, J. Cao, X. Jiang, S. Chen, "Cloud computing- based forensic analysis for collaborative network security management system". Tsinghua Science and Technology, 18, 40 - 50, 2013.

[12] K. Kourai, T. Azumi, and S. Chiba, "A self-protection mechanism against stepping-stone attacks for IaaS clouds", in Ubiquitous Intelligence & Computing and 9th International Conference on Autonomic & Trusted Computing (UIC/ATC), IEEE, pp. 539–546, 2012.

[13] M. Godfrey and M. Zulkernine, "A Server-Side Solution to Cache-Based Side-Channel Attacks in the Cloud", in Cloud Computing (CLOUD), pp. 163–170, 2013.

[14] Q. Yaseen and B. Panda, "Malicious Modification attacks by Insiders", in Relational Databases: Prediction and Prevention in Social Computing (SocialCom), pp. 215-218, 2010.

[15] M.T. Khorsheds, A.S. Ali, and S.A. Wasimi, "Monitoring insiders activities in cloud computing using rule based learning", in Trust, Security and Privacy in Computing and Communications (TrustCom), pp.900 -905, 2011.

[16] N. R. Potlapally, A. Raghunathan, S. Ravi, N. K. Jha, and R. B. Lee, "Aiding side-channel attacks on cryptographic software with satisfiability-based analysis". IEEE Trans. VLSI Syst.,15(4):465– 470, 2007.

[17] A. Duncan, S. Creese, M. Goldsmith, and J. S. Quinton, "Cloud computing: Insider attacks on virtual machines during migration," in Trust, Security and Privacy in Computing and Communications (TrustCom), International Conference on, Melbourne, Canada, July 2013.

[18] W. Lin and D. Lee, "Traceback Attacks in Cloud--Pebbletrace Botnet", International Conference on Distributed Computing Systems Workshops (ICDCSW), pages 493–500, 2012.

[19] K.O. Saputra, W.C. Teng, Y.H. Chu, "A Clock Skew Replication Attack Detection Approach Utilizing the Resolution of System Time", in IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), 2015.

[20] S. Zander and S.J. Murdoch, "An Improved Clock-skew Measurement Technique for Revealing Hidden Services", in 17th conference on Security symposium Pages 211-225, 2008.

[21] Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in Proc. A.C.M. MobiCom'08, 2008.

[22] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks", in Proceedings International Parallel & Distributed Processing Symposium, 2006.

[23] S. Kaplantzis, A. Shilton, N. Mani, and Y. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in Proceedings of Intelligent Sensors, Sensor Networks and Information, ISSNIP., Dec. 2007, pp. 335 – 340.

[24] M. Wazid, A. Katal, R.S. Sachan, R.H.Goudar, D.P. Singh, "Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network", International Conference on Communication and Signal Processing,, pp.576–581, 2013.

[25] Gao, H., Wu, R., Cao, M., & Zhang, C. (2014). Detection and defense technology of blackhole attacks in wireless sensor network. In Algorithms and architectures for parallel processing, Springer, pp. 601–610).

[26] S.Sharmila and Dr G Umamaheswari; "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms", International Conference on Process Automation, Control and Computing (PACC), pp. 1-6, 2011.

[27] J. Guo, Z. Lei, "A Kind of Wormhole Attack Defense Strategy of W.S.N. Based on Neighbor Nodes Verification", in International Conference on Communication Software and Networks, 2011.

[28] Y. Xu, Y. Ouyang, Z. Le, J. Ford, F. Makedon, "Analysis of Range-Free Anchor-Free Localization in a W.S.N. under Wormhole Attack", in A.C.M. Symposium on Modeling, analysis, and simulation of wireless and mobile

systems, Pages 344-351, 2007.

[29] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 5, Jun 2010.

[30] https://sorcloud.com/mathengine.

[31] R. Kumar Dwivedi, R. Kumar, "Sensor Cloud: Integrating Wireless Sensor Networks with Cloud Computing"," 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gorakhpur, India, 2018.

[32] Aditya Kumar Naik, Rajendra Kumar Dwivedi, "A Review on Use of Data Mining Methods in Wireless Sensor Network", International Journal of Current Engineering and Scientific Research - IJCESR (ISSN PRINT: 2393-8374, ISSN ONLINE: 2394-0697), Volume 3, Issue 12, 15 Dec, 2016, pp. 13-20.

[33] Arushi Agarwal , Surabhi Maddhesiya, Priya Singh and Rajendra Kumar Dwivedi, "A Long Endurance Policy (L.E.P.): An Improved Swap Aware Garbage Collection For NAND Flash Memory Used As

[34] A Swap Space In Electronic Devices", in "International Journal of Scientific and Engineering Research - IJSER (ISSN: 2229- 5518)", Volume 3, Issue 6, Pages 412-417, June 2012.

[35] Mukesh Kumar Chaudhary, Manoj Kumar, Mayank Rai, Rajendra Kumar Dwivedi, "A Modified Algorithm for Buffer Cache Management", in "International Journal of Computer Applications– IJCA (ISSN: 0975-8887)", Volume 12– No.12,Pages 47-52.

[36] Yuriyama, M., Kushida, T.: Sensor-cloud infrastructure-physical sensor manage-ment with virtualizedsensors on cloud computing (2010).

[37] Rajendra Kumar Dwivedi, Richa Tiwari, Daizay Rani, Samra Shadab, "Modified Reliable Energy Aware Routing Protocol For Wireless Sensor Network", International Journal of Computer Science & Engineering Technology - IJCSET (ISSN: 2229-3345)", Volume 3, No. 4, April 2012, pp. 114 – 118.

[38] R. Kumar Dwivedi, P. Sharma and R. Kumar, "Detection and Prevention Analysis of Wormhole Attack in Wireless Sensor Network," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2018, pp. 727-732.

[39] R. Kumar Dwivedi, S. Pandey and R. Kumar, "A Study on Machine Learning Approaches for Outlier Detection in Wireless Sensor Network," 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2018, pp. 189-192.

[40] Kishan Verma, Rajendra Kumar Dwivedi, "A Review on Energy Efficient Protocols in Wireless Sensor Networks", International Journal of Current Engineering and Scientific Research - IJCESR (ISSN PRINT: 2393-8374, ISSN ONLINE: 2394-0697)", Volume 3, Issue 12, 15 Dec, 2016, pp. 28-34.

[41] K. Verma and R. K. Dwivedi, "AREDDP: Advance reliable and efficient data dissemination protocol in wireless sensor networks," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2017, pp. 1-4.

[42] P. Sharma, R. K. Dwivedi, "Detection of High Transmission Power Based Wormhole Attack Using Received Signal Strength Indicator (RSSI)". In: Verma S., Tomar R., Chaurasia B., Singh V., Abawajy. (eds) Communication, Networks and Computing. C.N.C. 2018. Communications in Computer and Information Science, vol 839. Springer, Singapore.