An Analytical Survey of Various Learning Methods for IoT Based Privacy Preservation.

Pardeep Singh[1], Gaurav Aggarwal[2]
[1,2]Department of CSE, Jagannath University, Bahadurgarh, Haryana, India
singh.pardeep@gmail.com

Abstract: The Internet of Things (IoT) involves a network of Internet-connected gadgets that can detect, communicate, and respond to changes in their surroundings. Billions of these computer devices are linked to the Internet in order to share data with one another and/or with their infrastructure. The Internet of Things (IoT) aims to enable a multitude of smart services in practically every facet of our everyday interactions while also improving our general level of life. However, as IoT becomes more widely adopted, there are serious privacy worries about losing control over how our data is gathered and distributed with others. As a result, privacy is an essential prerequisite for every IoT ecosystem and a major barrier to mainstream consumer adoption. The ultimate source of consumer annoyance is the inability to regulate personal information in raw form that is directly transmitted.

Keywords: cloud computing, Machine Learning, Internet of Things,, Intrusion Detection, PSO

1. Introduction

The billions of devices that are linked to the Internet worldwide are collectively referred to as the "Internet of Things." The numerous tiny computers that are built into these gadgets allow them to communicate with one another and exchange data [1]. The limited processing resources of the Internet of Things are among its most significant characteristics. IoT edge data processing is typically required. Typically, edge devices are some form of embedded system. The processing power of embedded systems is minimal and constrained. Because of this, some methods for carrying out intricate and demanding IoT processing at the frontier] should be developed and distributed through sensors to the majority of the globe. The Internet of Things (IoT) has become a crucial part of our daily lives due to the rapid advancement of communication technologies as the IoT includes varied devices with limited connection, processing, and storage resources. The National Institute of Standards and Technology (NIST) has developed lightweight cryptographic algorithms for decryption and encryption, which are tailored to resource-constrained IoT devices. Authenticated encryption with associated data (AEAD) techniques provides encryption, integrity, and authentication in addition to confidentiality. While traditional encryption algorithms like AES only provide confidentiality, AEAD algorithms also provide authenticity [2].

In general, smart environments include smart cities as a subset. The integration of new technologies like IoT, AI, and big data analytics improves efficiency, sustainability, and habitability in many contexts. Interconnected smart items in every living location, not just metropolitan regions, create smart environments. The authors in [26] define a smart environment as a system that collects data about residents and the environment to model and adjust it. This idea fits the IoT goal . This vision envisions sensors and actuators collaborating to achieve common goals. The survey highlights significant IoT technology, applications, and potential advantages. Figure 1 displays the top smart settings based on expected IoT spending in 2020 and 2014-2020. The majority of expenditures were allocated to smart finance, transit, government/environment, customer experience, health, homes, energy, and manufacturing [31].

SDN-based IoT in automotive networks was proposed to identify DDoS assaults using properties from the latest benchmark dataset, BoT-IoT. NSW University researchers created the dataset. By selecting equal numbers of packets from every category, public data set concerns like mismatch and overfitting are solved. The authors in [32] have classified innocuous, reconnaissance, DoS, as well as DDoS traffic with 91% accuracy using ML and represented the derived characteristics in the dataset. This approach is unique since it uses the latest benchmarked data set and reduces malicious traffic identification characteristics by roughly half. They aim to improve feature comparison along with selection by using more benchmark data sets. Numerous avenues for research exist. This research might be expanded to test the ML model's efficacy with different subsets.

Machine learning (ML) and SDN are used to identify DDoS assaults. DDoS assaults continue to threaten network infrastructures and test traditional defenses due to their magnitude and sophistication. The authors in [33] have explained how SDN controllers monitor whole networks and ML models are linked to continually monitor and

analyze network traffic for DDoS detection. Compatibility with current infrastructure, choosing suitable ML algorithms like Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF), and KNearest Neighbor (KNN), and model training to adapt to changing threats are all challenges of SDN-based DDoS detection. This integrated strategy can increase network infrastructure resilience and reduce DDoS assaults on important services beyond mitigating immediate risks. These models are evaluated using recall, accuracy, precision, along with F1-score. On this UNB CIC-IOT 2023 dataset, the LR model outperforms SVM, RF, and KNN, with accuracy rates of 86%, 71%, 60%, as well as 65%, respectively.

The IIoT is being used in industrial activities including manufacturing and safety-critical control applications. The IIoT is complicated, with diverse hardware and software, interconnected sub-systems, and strict security, safety, and privacy standards[24]. Ensuring security and privacy in IIoT systems is challenging due to system complexity and difficulty in defining and proving security needs. The study aims to give a comprehensive overview of IIoT security and privacy, reflecting recommendations from reputable standardization groups. This will help academics and practitioners understand how different security protocols fit into the overall picture. A comprehensive review of security methods and solutions highlights risks and flaws. The study suggests future research areas to address IIoT security and privacy issues.

2. Literature Review

The necessity of privacy preservation is the growing integration of IoT devices using cloud computing. This study thoroughly examines privacy concerns at the confluence of IoT and cloud system. The extensive literature review [3] highlights significant difficulties and new developments in privacy-preserving approaches. Analyzing various methodologies reveals a deeper understanding of encryption, anonymization, access control, and the integration of AI. Recent trends include machine learning enabling dynamic anonymization, homomorphic encryption providing secure computation, and AI-driven access control. This survey provides a comprehensive overview of solutions for securing sensitive data in IoT-based cloud systems. This poll offers significant insights for those who are investigating and navigating privacy preservation in IoT and cloud computing.

Improving privacy in the AI-XR metaverse requires both technological and non-technical solutions[19]. To enhance privacy in the AI-XR metaverse, secure computing approaches can be used to handle sensitive data secretly. Use of HE is a mathematical method for safe computation. HE enables calculations on encrypted data without decryption. The computation is done on ciphertext and the result is also ciphertext, ensuring data privacy. To use HE in the metaverse, sensitive data must be encrypted before being sent to a server for execution.

Large amounts of useful industrial big data will result from Industrial Internet development. Companies can increase manufacturing efficiency, decrease costs and risks, optimize management processes, and create services and business models by mining and using IBD. Multiple institutions and diverse backgrounds contribute to IBD, which is multisource, heterogeneous, and multimodal. Data sharing and trading (DS&T) in the Industrial Internet lacks trust. Analytics and privacy/security technologies face new hurdles with these traits [4].

Federated learning (FL) offers a machine learning (ML) method that allows collective model training without disclosing raw data, making it perfect for IoT applications with scattered data and privacy concerns [5]. IoT systems depend on Wireless Sensor Networks (WSNs) to collect environmental data. This article covers FL, IoT, and WSN integration in detail. It explores FL basics, techniques, kinds, and FL, IoT, and WSN integration in many sectors. The study discusses FL heterogeneity issues and reviews current research. Security, privacy, and performance evaluation are also covered. FL, IoT, and WSNs' newest successes and possible research areas are discussed in the study, along with their importance in the context of contemporary technological advances.

Federated learning (FL) is an improved method for training machine learning (ML) models with dispersed data while protecting privacy and security. It allows collaborative model training across edge devices or servers without data transfer. Federated learning lets devices train on their own data instead of transferring it to a central server, which could endanger privacy[6]. These changes are incorporated to improve the global model over iterations. Data and user privacy concerns are rising with artificial intelligence (AI) becoming more widespread in new applications. FL advances are examined in this article, covering methodology, applications, and problems.

Everyday, massive data are generated exponentially. Analytics over data is necessary for meaningful insights nowadays. In essential applications, Big Data Analytics (BDA) makes good conclusions. Since local systems have massive data to process, cloud platforms store and process it. Public clouds are mostly third-party resources. Cloud privacy and security are top issues. Big Data has focused on secure and private BDA. The study [7] examines cloud BDA security and privacy solutions from the perspectives of safe access management, secure data storage, and private and confidential learning. Each component examines and presents techniques. Secure and private cloud BDA is the focus of this article. Challenges and possibilities for further study in this field have been outlined.

Rapid improvements in the Internet of Things (IoT) have revolutionized communication technologies and customer services. AI has been used to improve IoT operations and optimize their potential in modern applications[8]. The convergence of IoT and AI has created a new networking paradigm termed Intelligent IoT (IIoT), which might alter enterprises and industries.

Federated learning (FL) enables distributed machine learning on edge devices. However, the FL model creates privacy problems. Various methods, such homomorphic encryption HE, differential privacy, as well as multiparty collaboration solve FL model privacy concerns. HE offers enhanced security and privacy due to end-to-end encryption that protects data throughout computing. In contrast to other privacy-preserving methods, HE does not require a trusted environment or protocol among many participants, nor does it include artificial noise that might affect system performance. Unfortunately, it has efficiency overhead when used for privacypreserving FL (PPFL). Some surveys on PPFL include its design and organization, as well as real HE deployment in PPFL. However, none address optimizing HE efficiency in PPFL. The authors in [9] reviews HE efficiency enhancement for PPFL with a complete study and layout.

FL allows collaborative machine learning model training without sharing vulnerable local data. Traditional machine learning involves aggregating large amounts of raw data, posing privacy and security risks[10] . In 2016,the authors in [11] introduced FL, which trains models on local devices utilising private data and aggregates only local models, enhancing data privacy and avoiding central data collection.

At the start of FL, the parameter server distributes a global model with variables that are random across every participating clients. Clients train the model using local data and machine learning algorithms like gradient descent repeatedly. The parameter server updates the global model from each client's updated models after local training. The updated model is made available to clients for further training. This method is repeated unless the global model reaches the desired accuracy or completes the minimum amount of iterations.

The authors in [12] evaluate the risks of federated learning in real-life applications and suggest secure frameworks for mobile malware detection. They have examined the importance of federated learning in mobile OS, comparing machine learning and deep learning approaches for malware detection and explored the potential and challenges of in-built mobile operating system architecture and its impact on user privacy and security.

3. Security Challenges in Iot-Based Smart Environments

Evaluating the security of IoT-based smart environments, including smart homes and cities, is crucial for implementing proper controls and minimizing security risks. The challenge lies in identifying security standards and frameworks that meet requirements and thoroughly evaluate IoT-based smart environments' security posture. The authors in[20] have discussed existing security standards and review frameworks, including NIST unique publications on security techniques, to identify potential solutions for IoT-based smart environments. Overall, 80 ISO/IEC security standards, 32 ETSI standards, and 37 conventional security assessment frameworks, including 7 NIST special publications on security techniques, were reviewed. The review process included both published and developing security standards and assessment frameworks to provide comprehensive and current research. Most mainstream security standards and assessment frameworks cannot directly address IoT-based smart environment security needs, but can be adapted to do so. This study advances the IoT field by revealing current security standards and examining frameworks, enabling new research directions and development of new frameworks to address future smart environment security concerns. This paper addresses open issues and challenges in IoT-based smart environment security. This paper introduces taxonomy of IoT-based smart environment security challenges, based

on extensive literature review, and proposes potential solutions.

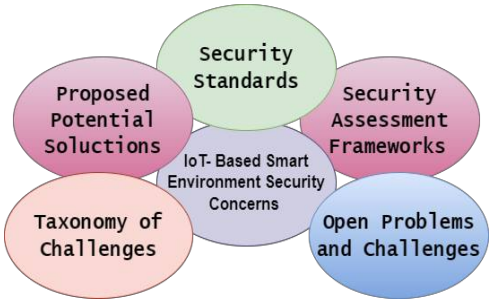

Fig 1: Key aspects of IoT security**.**

A network of individually identifiable embedded devices with embedded software to communicate across transitory states is the Internet of Things (IoT). The study by [22] aims to examine several IoT security problems related to current standards and protocols. This paper provides a comprehensive assessment of IoT security, including identifying threats, innovative protocols, and recent security efforts. This article provides an updated assessment of IoT architecture using protocols and standards for next-gen systems. To meet IoT security needs, protocols, standards, and security models are compared. This study highlights the necessity for communication and data audit standards to protect hardware, software, and data against risks and assaults. We found that procedures must be competent enough to address several threat vectors. This article explores current security research trends, which will benefit IoT security development. Research findings can benefit the IoT community by implementing optimum security features into devices.

Smart environments aim to increase human comfort and efficiency. The Internet of Things (IoT) is now a technology for creating smarter settings. Real-world smart environments based on the IoT concept prioritize security and privacy. The security flaws in IoT systems pose a danger to smart environment applications. Intrusion detection systems (IDSs) intended for IoT contexts are essential to prevent security attacks exploiting weaknesses. Conventional IDSs may not be suitable for IoT contexts due to restricted computation and storage capabilities and unique protocols. The article by the authors of [16] surveys the newest IoT-designed IDSs, focusing on their methodologies, features, and processes. This article offers a comprehensive understanding of IoT architecture, security vulnerabilities, and how it communicates with its levels. This study highlights the importance of establishing efficient, reliable, and resilient IDSs for IoT-based smart settings, notwithstanding earlier research on their design and implementation. This study concludes with key factors for developing IDSs as a future view.

IoT devices' open accessibility and lack of security have led to a rise in DDoS assaults. DDoS assaults may be launched against other targets utilizing the incursion, making it very susceptible. Attackers construct botnets by targeting several targets. The authors in [18] identified Confidentiality, Integrity, and Availability as the primary security concerns in IoT based networks. The authentication technique includes authenticating both data security and routing peers involved in data transfer. A major issue with IoT device authentication is key deployment and maintenance. The challenges of IoT compliance and security hinder the development of smart environments in the real world. DoS and DDoS assaults on IoT networks affect smart environment services. Communication security using the above protocols must be adequate. Information confidentiality, integrity, authentication, and non-repudiation must be satisfied by security mechanisms used to safeguard communications utilizing the listed protocols. The security of interactions with the Internet of Things may be analyzed inside the protocol stack. Denial-of-service attacks, unlike other attacks, progressively drain resources and network bandwidth, resulting in system shutdown without first symptoms of failure. The study by [15] covers DDoS defense techniques, including standard and IoT-specific approaches and focuses on DDoS assaults in IoT, in line with current developments. The role of IoT botnets and malware, including its novel variations, has been extensively examined to better comprehend the assault method. The variety of DDoS assaults is described by creating taxonomies for both attacks and defense methods. To compare the main defense systems in recent years, a category description is offered based on their system models, important features, and weaknesses.

IoT system security is a major concern as the number of services and users in these networks grows. By integrating IoT systems and smart surroundings, smart things become more effective. However, IoT security vulnerabilities pose significant risks in crucial smart environments in industries like health and manufacturing. In IoT-based smart environments, insufficient security puts apps and services at risk. Increasing research on information security in IoT systems is crucial to address problems of confidentiality, integrity, and availability in smart settings[17].

Security breaches are often caused by error by authorized users, rather than technological failures. Individuals can choose to reveal their matter in public [13]. Privacy might be mistaken with security and confidentiality. Confidentiality is a basic right rooted on privacy and informational self-determination, which pertain to personal data protection. Privacy refers to the fair and allowed processing as well as availability of personal information. Confidentiality goes beyond data protection rights (Table 1). Privacy must be disclosed before confidentiality may be legally "triggered" (first point). The right to privacy is a “negative” right since it prohibits interfering with private information. Privacy needs usually take two kinds. Organizations often develop privacy rules based on their ethical approach to managing information. Second, institutions and organizations must comply with various privacy laws and rules. Data security involves implementing logical, technological, administrative, and physical measures to guarantee data confidentiality, integrity, and availability. Confidentiality limits access to non-public information that has been agreed upon by many parties. Thus, confidentiality implies that sharing information with another person entails a promise not to share it with others.

Table 1: Components of Information Security**.**

Components	Definition	Role
Confidentiality	Information should not be shared with unauthorized persons, companies, or processes	Maintaining confidentiality is crucial for information security, since it restricts access to preserve personal privacy, and private knowledge
Integrity	Provides assurance that information is reliable, accurate, and has not been altered by unauthorized parties.	Integrity is essential for creating trustworthy information systems and preventing unwanted data changes.
Availability	To ensure authorized users have accurate and promptly access to information along with assets as needed.	Information systems require availability to function efficiently and provide data access when needed.
Authenticity	It confirms the identity of the sender or creator of the data and ensures that the message or data has not been tampered with during transmission.	Verification of Identity, Data Integrity and Secure Communication.
Non Repudiation.	It provides proof of the origin, delivery, and integrity of data, making it impossible for the sender or receiver to dispute their involvement.	Accountability. Auditability and Legal Compliance.

The intrusion detection system (IDS) software monitors and prevents malicious activities on a network. Intrusion detection detects unauthorized access to computer networks and information systems.

In contrast to exterior intruders, internal intruders are lawful users who attempt to escalate privileges to access illegal data or services within a network. IDS consist of a reporting system and a sensor. Sensors acquire data for its main purpose.

The authors in [14] suggest categorizing IoT IDS ideas based on the types of threats that can be discovered and detected. IoT systems may be exposed to security vulnerabilities from legacy technologies and middleware, including unsecured HTTP connections and malicious code injection, according to several writers. IoT IDS techniques fall into two categories: We concentrate on detecting DoS attacks and identifying routing assaults. Their findings suggest that both conventional and man-in-the-middle assaults pose dangers.

Smys et al. [27] emphasize the need of intrusion detection systems in current wireless networks due to poor security and more invaders. IoT networks require an intrusion detection system to prevent performance deterioration due to their heterogeneity and security risks, similar to wireless networks. The proposed research analyzed IoT threats and offered a hybrid convolutional neural network module with additional short-term memory. Through experimental testing, the proposed model achieves 98% higher detection accuracy than typical recurrent neural networks, making it suitable for many IoT situations. Depending on their purpose, IDSs can be host-based or network-based. A HIDS monitors a specific computer device for suspicious or malicious software components or unidentified programs that impact its operating system, whereas an NIDS analyzes aberrant network traffic. Additionally, IDS-described abuse or signature-based and anomaly-based network issues may be divided into two types. A misuse- or signature-based IDS hunts for compromised systems during assaults using signatures and patterns such network traffic byte sequences. Generally, IDS is needed at the communication level to monitor network activity and links, and generate alarms for anomalies, such as policy violations. Classic IDS methods often consider WSNs or the standard Internet, as mentioned by Mosenia and Jha [28]. IDSs can detect malicious nodes that inject misleading information or violate system rules. IDS-based injection issue solutions have been proposed in recent research efforts. Son et al. [29] developed a program that detects code injection attacks on servers with high accuracy.

1. IDS

Presently, several smart gadgets impact our surroundings and human existence. The rise of the Internet of Things (IoT) is enabling smarter business practices, including health monitoring, surveillance, flood mitigation, farming, as well as home automation, through improved connectivity [25]. Using IoT technology in smart surroundings enhances the accuracy of smart goods. Additionally, IoT networks face security risks such as DoS and DDoS. IoT solutions along with adaptive environments can be disrupted by these threats. The safety of the IoT ecosystem is a major concern. Firewalls, security software, and intrusion detection systems (IDS) are insufficient to protect systems against cyberattacks. Therefore, innovative AI algorithms like ML and DL are essential for enhanced security. IDS involves tracking and analyzing network data to respond to disruptive intrusions. Intrusion detection is a technique that identifies and analyzes data flow in networks.

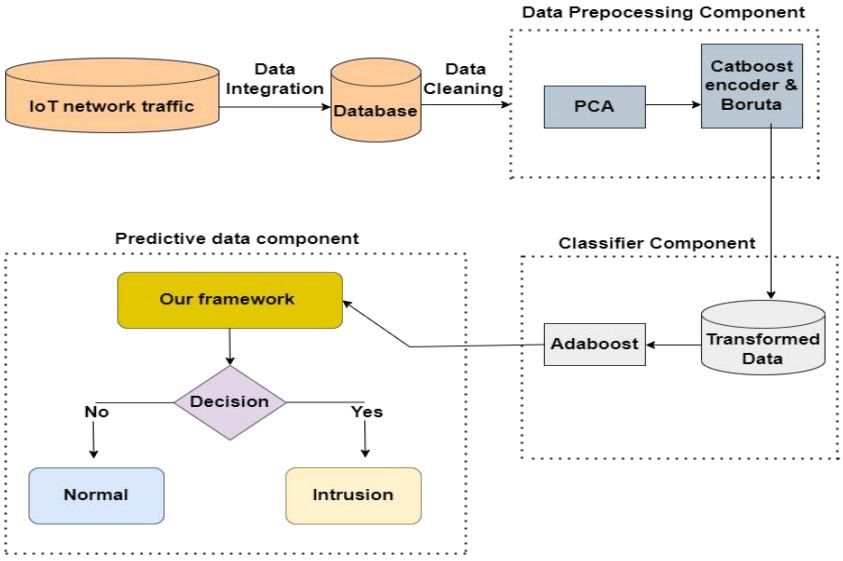

Fig 2: Block schematic of IDS

data preparation, classifier model, and predictive. The Boruta feature selection strategy, based on the xgboost boosting model, is used to pick the best features for data quality improvement. Second, Adaboost methods are used to generate a good IDS classifier model.

The intrusion detection system (IDS) software monitors and prevents malicious activities on a network. Intrusion detection detects unauthorized access to computer networks and information systems. While external intruders aim to access networks and/or information systems from outside the network, internal intruders are legitimate users who attempt to elevate privileges in order to get illegal data or services. IDS consists of a reporting system and a sensor. Sensors acquire data for its main purpose. The Internet of Things (IoT) provides high security for physical goods like intelligent machinery and home appliances. Physical items are assigned an Internet Protocol (IP) address for communication with external entities via the Internet. Increased hacker assaults during Internet data sharing put IoT devices at risk of security vulnerabilities. Effective attack detection is crucial for a dependable security system after powerful attacks. User-to-root (U2R), denial-of-service, and data-type probing attacks can affect IoT systems. This article presents performance-based AI models for accurate prediction of IoT device assaults and issues. Particle Swarm Optimization (PSO), genetic algorithms, and ant colony optimization were utilized to illustrate the efficiency of the recommended approach for four distinct parameters. The proposed PSO approach by [23] led to a 73% improvement over existing systems. Kennedy and Eberhart introduced the population-based global optimization approach of particle swarm optimization (PSO) in 1995[21]. It is inspired by the social behavior of birds flocking for food. PSO is a population-based search method. Individual swarm agents exhibit stochastic behavior due to their perception in the neighborhood, acting without supervision. Each particle in the swarm represents a solution in a high-dimensional space, with four vectors: current position, best position found, best position found by neighbors, and velocity adjusting based on best position reached by itself and neighbors (pbest and gbest).

The primary PSO benefits are: 1) PSO outperforms standard algorithms in processing speed and global searchability [30]. 2) Population size has little impact on training speed, as PSO doesn't seem sensitive to it. 3) The objective function can be optimized without calculating gradient information, and there are no limits on continuity, derivability, convexity, or connectedness of viable areas. PSO algorithm is described in Algorithm 1

5. Particle Swarm Optimization Algorithm (Pso)

Input:

N: Population size (number of particles)
pi: Local best position of particle i.
pg: Global best position (group optimal position)
fit: Fitness function to evaluate solutions

Algorithm for PSO

1. Initialize:

o Randomly initialize the position xi and velocity vi of each particle i in the search space.
o Set local best position pi←xi for all particles. o Determine the global best position pg based on the fitness values.

2. Repeat (until a stopping criterion is met, e.g., max iterations or a convergence threshold):

o For each particle i (from 1 to N):
1. Evaluate Fitness: Calculate fit(xi) using the fitness function.
2. Update Local Best:
   - If fit(xi)>fit(pi), then update pi←xi.

3. Update Global Best:

- If fit(pi)>fit(pg),then update pg←pi

4. Update Velocity and Position:

- Update the velocity vi using the formula: vi←w vi+c1 r1 (pi−xi)+c2 r2 (pg−xi) where:
- w: Inertia weight
- c1,c2: Acceleration coefficients (cognitive and social factors)
- r1,r2: Random values in [0, 1] ➢ Update the position xi: ▪ xi←xi+vi

3. End For Loop

4. Stopping Condition: Stop when the criterion is met (e.g., a max number of iterations, or minimal fitness improvement).

5. Return pg : The best solution found

6. Conclusion and Future work

Integrating Internet of Things (IoT) technology into daily life is rapidly growing and offers several benefits. Despite centralized security and authentication concerns including mining, hacking, and service denial attacks, blockchain technology offers a solution. However, powered by blockchain IoT systems face privacy issues that must be addressed before use.

Maintaining privacy in IoT contexts requires collaboration and cooperation from all stakeholders to ensure safety and enjoyment of its benefits. IoT device manufacturers must provide privacy and security features. Infrastructures should integrate IoT-based procedures to avoid privacy breaches and handle security risks. Users of IoT apps must be informed of the data gathered and its purpose. IoT users should exercise caution when granting access to private data and recognize the possible hazards of abuse.

References

1. Ahmadvand, H., Lal, C., Hemmati, H., Sookhak, M., & Conti, M. (2023). Privacy-preserving and security in SDN-based IoT: A survey. IEEE Access, 11, 44772-44786.
2. Tanveer, M., Chelloug, S. A., Alabdulhafith, M., & Abd El-Latif, A. A. (2024). Lightweight authentication protocol for connected medical IoT through privacy-preserving access. Egyptian Informatics Journal, 26, 100474.
3. Dhinakaran, D., Sankar, S. M., Selvaraj, D., & Raja, S. E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. arXiv preprint arXiv:2401.00794.
4. Liu, L., Li, J., Lv, J., Wang, J., Zhao, S., & Lu, Q. (2024). Privacy-Preserving and Secure Industrial Big Data Analytics: A Survey and the Research Framework. IEEE Internet of Things Journal.
5. Mengistu, T. M., Kim, T., & Lin, J. W. (2024). A Survey on Heterogeneity Taxonomy, Security and Privacy Preservation in the Integration of IoT, Wireless Sensor Networks and Federated Learning. Sensors, 24(3), 968.
6. Aggarwal, M., Khullar, V., & Goyal, N. (2024). A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training. Applied Data Science and Smart Systems, 570-575.
7. Amaithi Rajan, A., & V, V. (2024). Systematic survey: secure and privacy-preserving big data analytics in cloud. Journal of Computer Information Systems, 64(1), 136156.
8. Aouedi, O., Vu, T. H., Sacco, A., Nguyen, D. C., Piamrat, K., Marchetto, G., & Pham, Q. V. (2024). A survey on intelligent Internet of Things: Applications, security, privacy, and future directions. IEEE communications surveys & tutorials.
9. Xie, Q., Jiang, S., Jiang, L., Huang, Y., Zhao, Z., Khan, S., ... & Wu, K. (2024). Efficiency optimization techniques in privacy-preserving federated learning with homomorphic encryption: A brief survey. IEEE Internet of Things Journal, 11(14), 2456924580.
10. Chen, J., Yan, H., Liu, Z., Zhang, M., Xiong, H., & Yu, S. (2024). When federated learning meets privacy-preserving computation. ACM Computing Surveys, 56(12), 1-36.
11. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). PMLR.

12.]Nawshin, F., Gad, R., Unal, D., Al-Ali, A. K., & Suganthan, P. N. (2024). Malware detection for mobile computing using secure and privacy-preserving machine learning approaches: A comprehensive survey. Computers and Electrical Engineering, 117, 109233.
13. Nowrozy, R., Ahmed, K., Kayes, A. S. M., Wang, H., & McIntosh, T. R. (2024). Privacy preservation of electronic health records in the modern era: A systematic survey. ACM Computing Surveys, 56(8), 1-37.
14. Anand, N., Singh, K.J. (2024). A Comprehensive Study of DDoS Attack on Internet of Things Network. In: Swain, B.P., Dixit, U.S. (eds) Recent Advances in Electrical and
15. Electronic Engineering. ICSTE 2023. Lecture Notes in Electrical Engineering, vol 1071. Springer, Singapore.
16. Vishwakarma, R., Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun Syst 73, 3–25 (2020).
17. Elrawy, M. F., Awad, A. I., & Hamed, H. F. (2018). Intrusion detection systems for IoTbased smart environments: a survey. Journal of Cloud Computing, 7(1), 1-20.
18. Gendreau, A. A., & Moorman, M. (2016, August). Survey of intrusion detection systems towards an end to end secure internet of things. In 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud) (pp. 84-90). IEEE.
19. Anand, N., Singh, K.J. (2023). An Overview on Security and Privacy Concerns in IoTBased Smart Environments. In: Rao, U.P., Alazab, M., Gohil, B.N., Chelliah, P.R. (eds) Security, Privacy and Data Analytics. ISPDA 2022. Lecture Notes in Electrical Engineering, vol 1049. Springer, Singapore. [19]Alkaeed, M., Qayyum, A., & Qadir, J. (2024). Privacy preservation in Artificial Intelligence and Extended Reality (AI-XR) metaverses: A survey. Journal of Network and Computer Applications, 103989.
20. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEE Access, 9, 121975-121995.
21. Agarwal, S., Singh, A. P., & Anand, N. (2013, July). Evaluation performance study of Firefly algorithm, particle swarm optimization and artificial bee colony algorithm for nonlinear mathematical optimization functions. In 2013 fourth international conference on computing, communications and networking technologies (ICCCNT) (pp. 1-8). IEEE.
22. Rachit, Bhatt, S., & Ragiri, P. R. (2021). Security trends in Internet of Things: A survey. SN Applied Sciences, 3, 1-14.
23. Alterazi, H. A., Kshirsagar, P. R., Manoharan, H., Selvarajan, S., Alhebaishi, N., Srivastava, G., & Lin, J. C. W. (2022). Prevention of cyber security with the internet of things using particle swarm optimization. Sensors, 22(16), 6117.
24. Gebremichael, T., Ledwaba, L. P., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the industrial internet of things: Current standards and future challenges. IEEE Access, 8, 152351-152366.
25. Hazman, C., Guezzaz, A., Benkirane, S., & Azrour, M. (2024). Toward an intrusion detection model for IoT-based smart environments. Multimedia Tools and Applications, 83(22), 62159-62180.
26. Fährmann, D., Martín, L., Sánchez, L., & Damer, N. (2024). Anomaly Detection in Smart Environments: A Comprehensive Survey. IEEE Access.
27. Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC, 2(04), 190-199.
28. Mosenia A, Jha NK (2017) A comprehensive study of security of internet-of-things. IEEE Trans Emerg Topics Comput 5(4):586–602.
29. Son, S., McKinley, K. S., & Shmatikov, V. (2013, November). Diglossia: detecting code injection attacks with precision and efficiency. In Proceedings of the 2013 ACM SIGSAC conference on computer & communications security (pp. 1181-1192).
30. Liu, J., Yang, D., Lian, M., & Li, M. (2021). Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access, 9, 38254-38268.
31. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-thingsbased smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications, 23(5), 10-16.
32. Babbar H, Rani S, Driss M (2024) Effective DDoS attack detection in software-defined vehicular networks using statistical flow analysis and machine learning. PLoS ONE 19(12): e0314695.

33. Sharma, A., & Babbar, H. (2024, May). Machine Learning-based Threat Detection for DDoS Prevention in SDN-Controlled IoT Networks. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.
30. Liu, J., Yang, D., Lian, M., & Li, M. (2021). Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access, 9, 38254-38268.
31. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-thingsbased smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications, 23(5), 10-16.
32. Babbar H, Rani S, Driss M (2024) Effective DDoS attack detection in software-defined vehicular networks using statistical flow analysis and machine learning. PLoS ONE 19(12): e0314695.
33. Sharma, A., & Babbar, H. (2024, May). Machine Learning-based Threat Detection for DDoS Prevention in SDN-Controlled IoT Networks. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.