# PROJECT TITLE: SECURITY ATTACKS ON IOT NETWORKS

# NAME OF THE FACULTY: JAYASHREE J

## Team:

| Registration Number | Team Members |
|---|---|
| 20BDS0146 | Vennela G |
| 20BDS0167 | Pavan Saish |
| 20BDS0172 | Amogh A M |
| 20BDS0291 | Kolla Kranthi Priya |
| 20BDS0352 | Hari Priya A |

1. **Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network**

   This paper discusses the blockchain concept and relevant information that provide a detailed explanation of security attacks and provide solutions, it also includes blockchain security enhancement solutions by summarizing key points. Several attacks on blockchain and the security issues of blockchain with some real-world examples. Moreover, this paper discussed the various security issues, challenges, vulnerabilities, and attacks. Finally, we summarized existing security solutions for different environments and open research issues.

2. **A Survey on security attacks and solutions in the IoT Network**

   IoT devices collect user’s confidential data like browsing history,location,etc to make our daily life more convenient without human interaction paves way for many cyber security attacks like DDoS(Distributed Denial Of Service),spoofing,etc. Cyber security attacks may occur on the physical layer,network layer or application layer of IoT devices for which various solutions using machine learning, blockchain and edge computing are developed

### 3. Classifying Security Attacks in IoT Networks Using Supervised Learning

Machine learning models detect unauthorized activity, they are used in anomaly detection techniques for detecting abnormalities within the computer networks. In this paper, we use the Support Vector Machine(SVM) model to detect abnormalities. This model is trained and evaluated using both benign and malicious local sensor activity. The proposed detection model achieves up to 100% accuracy when evaluated with unknown data taken from the same network topology, and when blackholes, and sinkholes attacks are present, and 81% accuracy when operating in an unknown topology.

### 4. An Intrusion Detection System on Ping of Death Attacks in IoT Networks

In Ping of death attack, Attackers increase the length of transmit packets intentionally in order to degrade the network resources. The Intrusion Detection System(IDS) detects attack and filters over-length packets by minimising false alarm probabilities and maintaining missed detection probability below desired level. Simulation results state that the queue length is directly proportional to probability of the attack. Hybrid IDS has various modules for anomaly detection,misuse detection and decision-making with detection rate of 99.81%, false alarm rate of 0.57% and accuracy of 99.75%.

### 5. Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques

The Iot is currently facing many security threats than ever before so to resolve that Machine Learning(ML) algorithms have been used. In this paper the ML techniques are been segmented into two categories those are ML techniques and ML-based solution for IOT attacks detection. The ML solutions were used as three primary architectural layers of an IoT structure: the physical/perception layer, the network layer, and the web/application layer. ML based learning approaches may be used as an option for physical layer authentication. The authentication error has been decreased by 64.3 percent by QL-based learning methods. Supervised ML techniques such as Distributes Frank Wolf and incremental Aggregated Gradient are used to enhance the detection performance.

### 6. Analysing Adversarial Attacks Against Deep Learning for Intrusion Detection in IoT Networks

There are many security vulnerabilities that are going against IoT networks and they are being detected and handled by using the idea of deep learning techniques. The classification of penetration threats in IoT networks has been mostly performed by feedforward neural networks. In this study, we take a look at the Self-normalizing Neural Network, a FNN variation, and evaluate its effectiveness in identifying intrusion threats in an IoT network. The BoT-IoT dataset from the Cyber Range Lab of UNSW Canberra Cyber is used in our analysis. The FNN performs better than the SNN in the experimental findings for IoT networks intrusion detection based on multiple performance indicators including recall, precision, and accuracy in addition to multi-classification metrics like Cohen Cappas score.

## 7. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures

The major attacks are Distributed Denial of Service (DDoS), Man In the Middle (MITM) and reply attacks. This paper tells about the possible vulnerabilities in the modern IoT network. There are countermeasures for each and every attacks like for brute force Intrusion prevention system(IPS) is used, Malicious applications Anti-virus applications is used, back doors and exploits Intrusion Detction System(IDS) is used. Confidentiality, integrity must be present so for that cryptography implementation is necessary. The countermeasures present in this paper to overcome the security attacks in the IoT are Intusion Prevention system(IPS), virtualization, Defense mechanism, proper authentication, antivirus applications and intursion detection system(IDS).

## 8. Identifying the attack surface for Iot networks

Iot devices consists of the integrated objects ,computations=al devices and soon…these do not need the human interaction,operation was made independently with the with the existing infrastructure.As the devices increases the threats and the issues will be increased.Here the threat model is increased with systematically finds the solution for the security issues.Creating the Iot infrastructure and breaking it into various can concentrate more on the vulnerabilities and weakness with the unauthorised users.Attack surface is the sum of all penetrations also known as vectors.

## 9. Deep learning-based intrusion detection for Iot networks

Due to the various constrained resources and limited computational capabilities,Iot networks are prone to various attacks.Novel intrusion detection system which classifies the traffic flow through the deep learning concepts.Binary and multiclass model of feed forward neural network are used for the classification of denial of services .Capability of binary classification for DDoS/DoS attacks are attacks were demonstarted by the result close to 0.99 considers evaluation measures including accuracy ,precision,recall and F1 score.In multi-class classification the accuracy level is 0.98 for DDoS/DoS attacks.

## 10. LiDL:Localization with early detection of sybil and wormhole attacks in Iot network

Dealing with the major security threats and risks for RLP based Iot networks.Two algorithms were proposed to overcome the security attacks caused for the sybil and wormhole.These benefit the HRCA concept which considered the local ancestors to perform the detection process.The feasibility of our algorithms are assessed by the sent of rules,which considers the algorithms as the light weighted,scalable and effective.Network detection used LLN's in the starting stage,future it concentrates on the RLP based Iot networks.Intrusion detection system is build to identify and mitigate various attacks and thus improves the network security.

## 11. Federated Learning-based Anomaly Detection for IoT Security Attacks

This paper suggests employing decentralised on-device data in a federated learning (FL)-based anomaly detection strategy to better detect intrusion in IoT networks. The data is kept intact on local IoT devices using our method, which employs federated training cycles on Gated Recurrent Units (GRUs) models and only shares the learned weights with the FL's main server. The ensemble component of this method combines the updates from several sources to enhance the accuracy of the overall ML model. Our test results show that our method secures user data privacy better than traditional/centralized machine learning (non-FL) versions and offers the best accuracy rate for attack detection.

## 12. Integrating complex event processing and machine learning :An intelligent architecture for detecting Iot security attacks

The rapid increase in the Iot devices had a challenge which detects and combating the cyber attacks and threats,including malware,security breach.To solve this challenge this paper proposes an architecture which integrates complex event processing (CEP) technology and machine learning paradigm to detect attacks. A model-driven graphical tool for the security pattern definition and automatic code is provided.This is useful in healthcare centers to find the malicious devices.Architecture was proposed using CEP and ML.Integration of CEP and Ml has many benefits.Iot network prototype is constructed in the hospital with the aim of detecting attacks.

## 13. Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures

Security in IoT devices and Wireless Sensor Networks(WSN) that creates an open avenue to attackers for intrusion are: absence of dedicated infrastructure such as gateways to watch flow of information in the network , recent integration and collaboration of WSNs with IoT and low-level security. The solutions to defend against security attacks consist of Prevention, Detection and Mitigation constitute a whole security structure. Intrusion Detection System technique which requires high processing power is also efficient against zero-day attack

## 14. Investigating Brute Force Attack Patterns in IoT Network

End nodes (sensors/devices) are attached to IoT networks and communicate with a data/application server through a gateway. The collected data is usually transmitted from the gateway to data server through a FTP server. Unfortunately, the security protocols enforced here are often not properly setup. The unique characteristic of this paper is that it incorporates a time-sensitive statistical relationship approach and visualising the attack patterns that identify themselves as brute force attacks when we study their features. This paper investigates brute force attacks that try to gain escalating privileges on an FTP server on the IoT network.The snort analysis done on the captured data provides information to the system administrator in the form of a warning alert to report network occurrences.

### 15. Efficient and Intelligent Attack Detection in Software Defined IoT Networks

In this paper, we explore effective software-defined IoT (SDIoT) network threat detection methods. In order to mimic common attacks like SYN, ping flood, UDP port scan, and UDP flood for a particular SD-IoT architecture, researchers first use MininetWiFi to gather representative datasets using Wireshark. The impact of various feature sets like IPs & ports on the detection accuracy for multiple attacks are then studied, with the use of Random Forest machine learning models. Moreover, where the run-time overheads can be greatly reduced, the detection accuracy of RF only modestly declines with smaller forests. This enables the strategies to function in IoT networks with limited resources.

### 16. Attacks and Defenses in Short-Range Wireless Technologies for IoT

This paper contains IoT uses various connection technologies to connect billions of diverse objects, or Things and offers end users from all over the world a range of application domains. In terms of diversity, scope, and use cases, Iot has came up with very new upgradation. The most prevalent, significant, and vulnerable component of the IOT is still believed to be the wireless infrastructures.In this work, researchers present an overview of attacks against IoT wireless infrastructures generally, and specifically against the most popular short-range wireless communication technologies in the IoT's resource-constrained domain. We specifically take into account the wireless communication technologies Wi-Fi, Bluetooth, ZigBee, and RFID.

### 17. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey

Classical encryption techniques should be used for the data security of the IoT network. The rule based approaches and deep machine learning algorithms-branches of artificial intelligence can be employed as the countermeasures. This paper presented a comprehensive layer-wise survey on IoT security threats, and the AI based security models to overcome the security attacks. There are different types of threats, they are Perception layer threats, network layer threats, transport layer threats, processing layer threats and application layer threats. This paper provides the features of different ML and DL approaches. Rule based ML and shallow ML is being used. Among all DL applications, ANN, CNN, RNN, Autoencoder etc are more prominent to handle various threats in IoT networks. Several new learning methods and novel visualisation techniques will be important for accurate data comprehension.

### 18. IoT network attack detection and mitigation

This paper describes and assesses a distributed and reliable system for detecting and preventing attacks in network environments where Graph Neural Networks are used by communicating decision agents to send out assault warnings. Researchers also describe an attack mitigation system that processes alarms issued by the attack detection system, along with Quality of Service metrics, to re-route sensitive traffic away from vulnerable network channels and this is powered by reinforcement learning. In this paper the detection and re-routing strategies are demonstrated by experimental findings. It also gives us an pre avoidance methods that are mentioned in future work.

### 19. Identification of cyber attacks using machine learning in smart IoT networks

The demand and usage of IoT are expanding rapidly. Several organisations are funding in this domain for their business use and giving it as a service for other organisations. The result of IoT development is the rise of different security difficulties to both organisations and buyers.This paper proposes, Machine-learning algorithms that can be applied in different ways to limit and identify the outbreaks and security gaps in networks.The main focus in this paper is the analysis of performance of these Machine learning algorithms when opposing network-related cyber security assaults,with specific focus in Denial of Service attacks. The dataset here holds a lot of separate bits of data but that can be used to instruct an algorithm to detect expected patterns inside the entire dataset.Massive metadata is required to detect various cyber security attacks.The dataset utilised here is Bot-IoT dataset.

### 20. Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks

The wide dispersion of the Internet of Things (IoT), Software-defined Networks and Cloud Computing have given the wings to Cyber–Physical System adoption. The newfangled society relies so much on Cyber–Physical Systems.The IoT devices are unwittingly contributing to the denial of service attacks. Though the neoteric Software-defined Anything (SDx) paradigm has offered effective solution approaches to catastrophic IoT-based DDoS attacks.In this paper, we present a comprehensive survey on vulnerability analysis of security solutions for Software-defined Cyber–Physical System., Cyber–Physical Systems are a confluence of physical systems (viz. Distributed Sensors, Mobile Systems, Embedded and/or Real-time systems) coupled to cyberspace to form a CPS ecosystem.In this paper, we have studied and examined the state-of-theart Cyber–Physical System, components of modern-day Cyber– Physical System, architectural details, security issues with a focus on most devastating DDoS and IoT-DDoS attacks.

### 21. The acceptance of Internet of Things (IoT) applications and services has seen an enormous rise of interest in IoT.

Smart city is an ongoing area of research where different technologies are used to make cities more sustainable. Internet of Things (IoT) is one of the emerging technology based on interconnected sensing and communication enable autonomous machines, instruments, sensors, robotic devices and actuators. An IoT network is implemented in industries, these connections experience various challenges including connection losses, slow communication,energy consumption etc. These may be the result of a malicious attack by a third party. Some of these attacks are f Hello-Flood attack, version number attack, sinkhole attack and black hole attack in RPL protocol. This paper proposes a framework that detect the presence of these threats and it also gives the design and architecture of these algorithms.A novel and secure framework are proposed for RPL based resource constraint large scale IIoT environments. The proposed framework consists of two phases, threshold modulation phase, and attack detection phase to cater to some common attacks in RPL based networks.

### 22. IoT Security: Botnet detection in IoT using Machine learning

The acceptance of Internet of Things (IoT) applications and services has seen an enormous rise of interest in IoT.The overwhelming amount and ubiquitous presence have fascinated potential hackers to organise cyber attacks and data theft. The key proposal of this paper is an innovative machine learning algorithm to detect and mitigate botnet-based distributed denial of service(DDoS) attacks on IoT networks.Our proposed model uses K-Nearest Neighbour(KNN) Naive Bayes model and multilayer perception Artificial Neural Network.The developed model is trained over a BoT-IoT dataset and the algorithm with the greatest accuracy is selected. By the experiment we conclude that KNN classifier is the most efficient for botnet detection in IoT networks.

### 23. Intrusion Detection in IoT Networks Using Deep Learning Algorithm

This paper proposes various machine learning and deep learning strategies and as well as standard datasets for improving the security performance of the IoT. A deep learning algorithm is developed for detecting denial-of-service(DoS) attacks.On experimenting we found that Random forests and CNN provides best results in terms of accuracy and AUC for multiclass classification. We found that increasing the batch size could speed up the calculation process.

### 24. IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework

In this paper, we first carry out an analytics approach to review security risks associated with IoT systems, and then propose a machine learning-based solution to characterise and detect IoT attacks. We take a real world IoT system with secured gate access as a platform,We study all the features of the system related to threats/attacks in detail.This system is observed over a period of nine months, And data is collected from this and used as our training data. We evaluate the efficiency of the machine learning models and propose a loose framework for implementing security in the respective IoT system.This paper illustrates the importance of the aspects of the framework which guide the model to accurately detect network layer and application layer attacks from normal traffic.It can differentiate different types of network layer attacks.

### 25. An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks

Recently, IoT infrastructures are vulnerable to specific cyber attacks. These cyber attacks are formed by slightly mutating the pre-existing attacks to mask them as routine traffic through an IoT network. In this paper, a new and comprehensive intelligent and autonomous deep learning identification and classification system is proposed which used Convolutional Neural Networks(IoT-IDCS-CNN). The dataset used here is NSL-KDD,which includes all key attacks found in IoT networks. The proposed system has,detection accuracy of 99.3% between normal or anomaly and it classifies the given IoT traffic into five categories with accuracy of 98.2%.

# References

[1] Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutionsfor the future distributed iot network. IEEE Access, 9, 13938-13959.

[2] Liang, X., & Kim, Y. (2021, January). A survey on security attacks and solutions in the IoT network. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0853-0859). IEEE.

[3] Ioannou, C., & Vassiliou, V. (2019, May). Classifying security attacks in IoT networks using supervised learning. In 2019 15th International conference on distributed computing in sensor systems (DCOSS) (pp. 652-658). IEEE.

[4] Abdollahi, A., & Fathi, M. (2020). An intrusion detection system on ping of death attacks in IoT networks. Wireless Personal Communications, 112(4), 2057-2070.

[5] Haji, S. H., & Ameen, S. Y. (2021). Attack and anomaly detection in iot networks using machine learning techniques: A review. Asian journal of research in computer science, 9(2), 30-46.

[6] Ibitoye, O., Shafiq, O., & Matrawy, A. (2019, December). Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In 2019 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

[7] Rajendran, G., Nivash, R. R., Parthy, P. P., & Balamurugan, S. (2019, October). Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[8] Rizvi, S., Orr, R. J., Cox, A., Ashokkumar, P., & Rizvi, M. R. (2020). Identifying the attack surface for IoT network. Internet of Things, 9, 100162.

[9] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019, December). Deep learning-based intrusion detection for IoT networks. In 2019 IEEE 24th pacific rim international symposium on dependable computing (PRDC) (pp. 256-25609). IEEE.

[10] Kaliyar, P., Jaballah, W. B., Conti, M., & Lal, C. (2020). LiDL: localization with early detection of sybil and wormhole attacks in IoT networks. Computers & Security, 94, 101849.

[11] Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated-Learning-Based Anomaly Detection for IoT Security Attacks. IEEE Internet of Things Journal, 9(4), 2545-2554.

[12] Roldán, J., Boubeta-Puig, J., Martínez, J. L., & Ortiz, G. (2020). Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. Expert Systems with Applications, 149, 113251.

[13] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[14] Stiawan, D., Idris, M., Malik, R. F., Nurmaini, S., Alsharif, N., & Budiarto, R. (2019). Investigating brute force attack patterns in IoT network. Journal of Electrical and Computer Engineering, 2019.

[15] Zhang, Y., Xu, J., Wang, Z., Geng, R., Choo, K. K. R., Pérez-Díaz, J. A., & Zhu, D. (2020, December). Efficient and intelligent attack detection in software defined IoT networks. In 2020 IEEE International Conference on Embedded Software and Systems (ICESS) (pp. 1-9). IEEE.

[16] Lounis, K., & Zulkernine, M. (2020). Attacks and defenses in short-range wireless technologies for IoT. IEEE Access, 8, 88892-88932.

[17] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access, 9, 94668-94690.

[18] Gelenbe, E., Fröhlich, P., Nowak, M., Papadopoulos, S., Protogerou, A., Drosou, A., & Tzovaras, D. (2020, June). IoT network attack detection and mitigation. In 2020 9th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-6). IEEE.

[19] Malathi, C., & Padmaja, I. N. (2021). Identification of cyber attacks using machine learning in smart IoT networks. Materials Today: Proceedings.

[20] Snehi, M., & Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks. Computer Science Review, 40, 100371.

[21] Qureshi, K. N., Rana, S. S., Ahmed, A., & Jeon, G. (2020). A novel and secure attacks detection framework for smart cities industrial internet of things. Sustainable Cities and Society, 61, 102343.

[22] Pokhrel, S., Abbas, R., & Aryal, B. (2021). IoT security: botnet detection in IoT using machine learning. arXiv preprint arXiv:2104.02231.

[23] Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. Information, 11(5), 279.

[24] Wheelus, C., & Zhu, X. (2020). IoT network security: threats, risks, and a data-driven defense framework. IoT, 1(2), 259-285.

[25] Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics, 9(12), 2152.