A Layer based Aspect of the Security Issues in Internet of Things: An Analytical Survey.

Pardeep Singh[a] and Gaurav Aggarwal[b]

[a] Research Scholar, Department of CSE, Jagannath University, Bahadurgarh, Jhajjar (Haryana)

[b] Professor, Department of CSE, Jagannath University, Bahadurgarh, Jhajjar (Haryana)

Abstract: A new paradigm known as the Internet of Things (IoT) makes it possible for a large number of devices to be continuously connected and enables for remote management of these things. These days, the Internet of Things has become taken for granted in our daily lives. These connected devices routinely collect and save user personal data online. These days, one of the main concerns is how collected data is protected. As devices grow increasingly interconnected, privacy and security problems have grown in significance and need to be addressed right away. Much study has lately been done on ways to defend IoT devices in an attempt to relieve customers' security anxieties, as attacks have the potential to damage consumer security and privacy. Blockchain technology research has been conducted to address security and privacy concerns related to IoT data collecting. This research aims to raise awareness about the privacy and security issues found in Internet of Things developments. The article aims to achieve this by analyzing security challenges at every level of the protocol stack, identifying relevant security requirements as well as fundamental issues, and providing an overview of the security measures that have been put in place to protect the Internet of Things (IoT) from its complex environment. IoT devices and implementations, which could have an impact on how these technologies are used in real-world scenarios.

Keywords: Buffer Overflow attack, CIA triads, DoS, DDoS, Hello Flood, IoT Security, Sinkhole.

INTRODUCTION

Scholars are starting to adopt the Internet of Things, or IoT, more frequently. Even in the lack of interpersonal communication, it enables everything to be connected to the other things via the internet. These devices have established an exclusive addressing scheme that allows them to communicate with each other in order to construct applications as well as services such as smart cities, smart transportation, and smart homes, among many more [1]. There are several security as well as privacy issues because of the Internet of Things' broad, intricate, and varied nature [2].IoT security's main goal is to safeguard the sensitive data from unwanted access. The well-known CIA triangle typically serves as the focal point of the security features. The CIA triad is another name for it.The CIA triad typically consists of Confidentiality, Integrity as well as Availability, as seen in Fig 1. The CIA triad is a paradigm for implementing security rules in diverse organizations. Big sensing data streams are primarily sourced from IoT. Big data streams are becoming an important area of research for the devices with fixed resources, however security issues with big sensing data streams remains up for debate. The study conducted by the authors in [18] provides a brief retrospective of the big data flow security classification in respect to IoT architecture. Emphasis is placed on the principles of cybersecurity threats and potential solutions for settings with massive data streams. Ultimately, the study classified the security concerns using the CIA (confidentiality, integrity, and availability) triad.

Confidentialit
y
Integrity
Availability

Fig. 1. CIA Triad for Data Security

Confidentiality is an ensemble of guidelines that restricts access to data. It shields the sensitive data from illegitimate access. It not only helps to keep the information hidden, but it also helps to avoid disclosure vulnerabilities.

Data integrity entails the accuracy and consistency of data. All appropriate precautions must be taken to guarantee that unauthorized individuals do not modify data. It also protects against forgery, subversion, as well as masquerade attacks.

Availability: As the name implies, the data ought to remain available to the appropriate user(s) whenever they need it. It aids in the prevention of Denial of Service (DoS) attacks. Table 1 highlights the various possible threats under the CIA triad.

TABLE I. POSSIBLE THREATS OF IOT GENERATED CIA TRIADS.

Confidentiality	Integrity	Availability
Access Authorization [28]	Sinkhole	Risk based Access Control
Traffic Analysis	Sybil	Role based Access Control
Eavesdropping	Wormhole	Encryption based Access Control
Attack Against Privacy	Acknowledgement Spoofing	Proximity based Access Control
Camouflage adversaries	Hello Flood	View based Access Control

A. Sinkhole Attack

Attacks at the Network Layer include sinkhole attacks. The attack is still going on. As a result, the network's performance gradually declines. This is not the same kind of attack. The source and destination nodes that will be the target of the assault are first selected by Sinkhole [21]. The hostile node in this attack (shown in fig. 2) draws traffic. By using compelling strength or data transmission power to declare a false ideal path, the hostile node attracts the fascination of the nodes nearby. Due to information sharing between fooled neighbors and hostile or malicious nodes, the malicious node drops packets. Blackholes, selective forwarding, eavesdropping, and other attacks can all benefit from the sinkhole attack, among others.

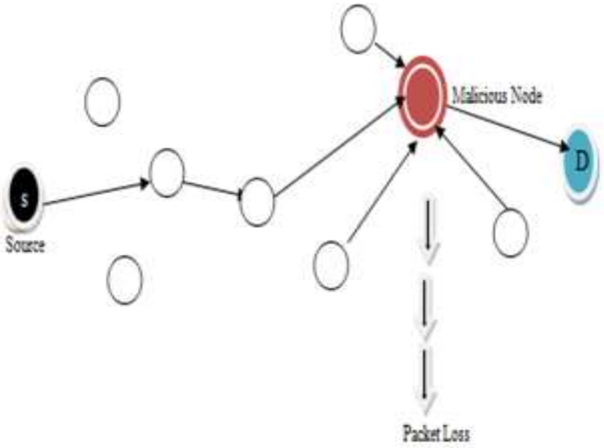

Fig. 2. Sinkhole Attack.

B. SybilAttack

Here the attacker impersonates to be multiple persons simultaneously. It manipulates the network and controls it by making multiple fake profiles. In fig 3,D represents the Malicious node and(X, Y, Z) represents Sybil nodes. If D interacts with any distinct nodes in the network by fake identity, it is enough for the legitimate node to create confusion to whom it is interacting with. The legitimate user will think that it is interacting with 4 nodes whereas in reality there is only one node with three multiple fake nodes[19].

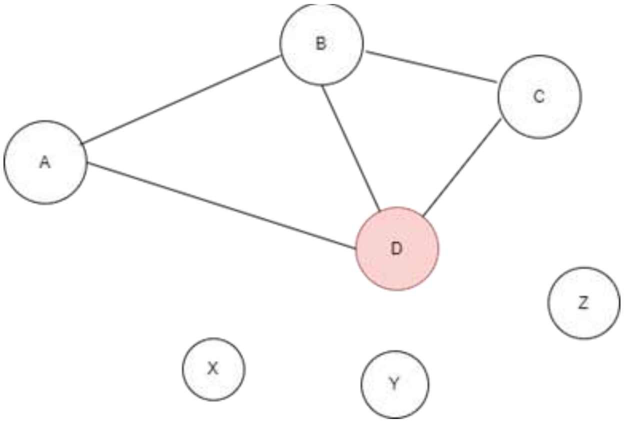

Fig. 3. Sybil Attacks

C. Wormhole Attack

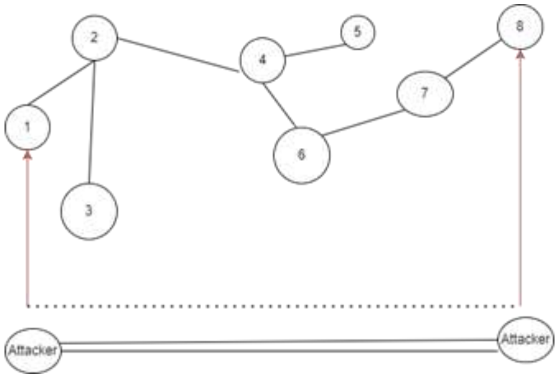

Fig. 4. Wormhole Attack

A significant attack called a wormhole attack [20] is made up of two attackers that place themselves strategically inside the network and then listen to as well as record wireless data from the network. Both attackers are situated in a key important area of the network, as seen in Fig**4**. The attackers positioned themselves in a network in a strong strategic position. They take use of their placement, which is to say that they have the shortest path among the nodes. To let other nodes over the network know they have the quickest route for delivering their information, they make their route public. The wormhole attackers build a tunnel for recording the current communications along with traffic at a particular position and channel them to an additional location within the network.

D. ACK Spoofing:

Few routing Protocols use link layer acknowledgements. Here the attacker may spoof the acknowledgments. This type of attack convinces that weak link is strong or dead link is alive.[16]

TABLE II. ACK FRAME FORMAT

2 Bytes	2 Bytes	6 Bytes	4 Bytes
Frame Control	Duration	Receiver Address	Checksum

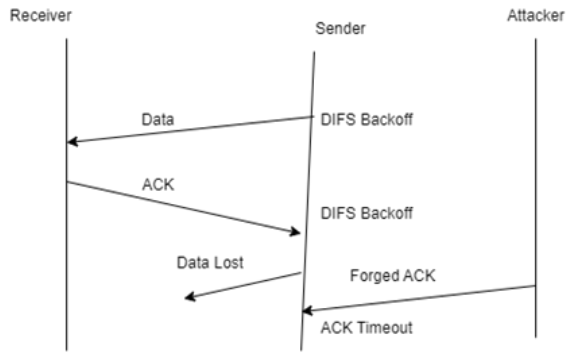

Fig. 5. ACK Spoofing

The frame control field, that is detected in a 14-byte-long ACK frame, shown in Table. II, specifies the frame kinds, control management and contents. The duration field tells surrounding nodes how long the channel was occupied; for ACKs, this field is usually 0. The receiver address argument indicates where the ACK is located. The checksum field is suitable for detecting any corruption in the transmission. The data sender cannot confirm the authenticity of the ACK frame based only on these four characteristics.

The different ways an attacker could launch an attack are described in Fig 5. If the distance involving the sender as well as the receiver is higher than the distance involving the sender as well as the attacker, the sender may raise the transmission rate since it hasn't been the highest previously. In this scenario, the attacker can fabricate an ACK for tricking the sender into thinking the channel strength is acceptable. Nevertheless, throughput will deteriorate (or cease to exist) when the channel state is unable to sustain the higher rate due to frame losses.

E. Hello Flood Attack.

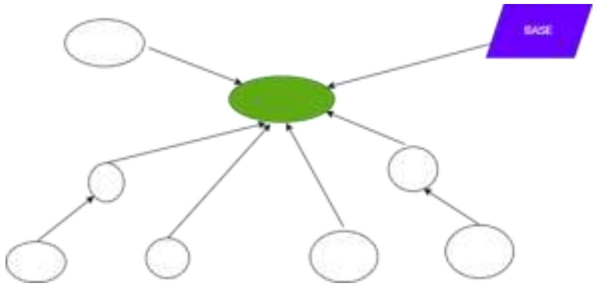

Fig. 6. Hello Flood Attack

A hello flood attack is the main attack at the network layer. As evident from Fig 6, a node which broadcasts a Hello packet so strongly that a sizable number of nodes, regardless of how who are miles away in the network, recognize it as its parent node, can start a hello flood attack [22]. A network layer attack that targets routing systems is comparable to the HELLO flooding attack. The protocols demand that the nodes that transmit HELLO packets should let the corresponding nodes about their presence. A node is referred to be the local node after accepting a data packet from another node inside its coverage area. Here, a routing system utilizes the nodes to communicate with neighbors by sending greeting messages.

II. Literature Review

According to Guillemin and Friess [3], the Internet of Things (IoT) enables users to connect with anything and anybody at any time, from anywhere, utilizing any path, network, or service. According to figure 8.[4] Explains a number of important aspects, such as intelligence, large scale, sensing, the environment, heterogeneity, and enormous data. For hastening the introduction of IoT, the IoT reference model as stated in [5] was introduced. Considering the dynamic nature of the system, security is a significant concern. [6] Discusses the capability of the gadgets to link with one another. IoT is the idea of ubiquitous connection, where practically all things have Internet Protocols (IP) built in, allowing them to connect to one another over the internet [7]. These objects can exchange the information using the unique identifiers, over various networks constituting a large IP based network of interconnected things [8]

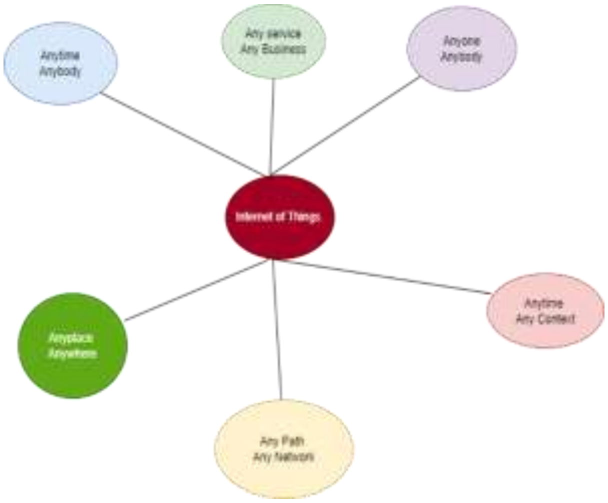

Fig. 7. Interconnecting IoT

On occasion, security is perceived as a distinct component of a system's architecture, with a separate module responsible for providing security. This division, however, is generally not a good approach to network security [14]. Due to the fact that components built without security can serve as entry points for threats, security requirements must be incorporated into each component to produce a secure system. Therefore, it is imperative that security measures permeate each aspect of system architecture.

One critical undertaking during the construction of a sensor network is the generation of cryptographic keys for subsequent use. Due to the inherent properties of sensor networks, earlier protocols were impractical. Public-key cryptography (e.g., Diffie-Hellman key exchange) surpasses the capabilities of existing sensor networks.

IoT devices must adhere to stringent dimension and power specifications and provide uninterrupted communication. Network availability is a vital variable determining the quality of service (QoS) it provides. The researchers in reference [13] detail a sequence of uncomplicated experiments designed to examine the effects of Denial of Service (DoS) on a sensor node of the Internet of Things (IoT) that is transmitting data to the cloud. The forthcoming implementation of an IoT sensor node was formulated based on the findings obtained from their experiment. Their objective is to establish a robust research foundation by revealing the negative consequences of DoS attacks upon IoT sensor nodes through experiments. The results indicate that DoS significantly impacts the network availability and power consumption of IoT sensor nodes.

III. TAXONOMY OF DDOS ATTACK IN IOT

Denial-of-service (DoS) attacks operate distinctively from different kinds of attacks in that the targeted device is usually not shown significant early indications of failure. Rather, they gradually deplete every resource, consuming all network bandwidth, and finally bringing about a server's shutdown. The concepts of DDoS attack defense have been discussed by the writers in [30], who have addressed both traditional and IoT-specific strategies. But similar to recent advances, they have concentrated their research on DDoS attacks in the Internet of Things—more precisely, on how malware and botnets operate in the IoT. The vast range of DDoS attacks is explained by creating categories on DDoS attacks as well as DDoS defense strategies.Denial of Service (DoS) attack is a cyber-attack in which the attacker tries to make the resource unavailable by consuming the resource or bandwidth of the legitimate user. Here a single machine is used to launch an attack without any involvement of malware whereas a cyberattack known as a Distributed Denial of Service (DDoS) occurs when different sources start the incoming traffic. In comparison to a DoS attack, it is more complex and challenging to defend against. To target the machines, it employs malware.

Given that DDoS attack detection is essentially an interconnected issue, which involves a reliable distributed solution is preferred. A DDoS prevention technique shouldn't interfere with the actions of legitimate users [27]. The security components of a defense system must protect against external and internal risks that could facilitate DDoS attacks which are launched within a network. Defensive systems that can be deployed and scaled should be rewarded financially. Rather than being a one-size-fits-all solution to every problem, defense should be planned to be incorporated into a bigger solution over time. DDoS (Distributed Denial of Service) is currently a major security concern, according to authors in [24]. The primary causes and consequences of DDoS assaults were examined by the writers in [25]. They used a GA learning technique to train an MLP to recognize DDoS attacks by examining the volume of entropy generated by the searches, the variance in entropy, and the amount of HTTP GET requests. It was shown that entropy was more beneficial when interacting with regular clients and less beneficial while speaking with attackers [29]. They also found that the likelihood of a client attack is essentially nonexistent. It indicates that throughout the attack, a specific number of HTTP GET requests being sent. The proposed method possesses a sensitivity of 0.9962, specificity of 0.9962, with accuracy of 98.32% against DDoS attacks.

There exist two types of DDoS attacks namely Bandwidth Depletion Attack and Resource Depletion Attack.

A. *Bandwidth Depletion Attack*

This attack consumes victim's bandwidth and floods the unwanted traffic and prevents the legitimate traffic to arrive at the victim's network. Generally, these attacks are carried by tools like Trinoo.

B. *Flood Attack*

In this scenario, the zombie overwhelms the victim's workstation with a huge amount of IP traffic, causing the system to either slow down or crash as a result of the excessive workload[23]. The attacker employs two methods: flooding the server with a substantial volume of bandwidth to generate fake activity, or obstructing real users from accessing services and making requests by overwhelming the network with an excessive quantity of data, causing congestion. Flooding attacks can manifest in various forms. Some examples of flooding attacks are address spoofing based data flooding attack (ASDF), non-address spoofing based route request flooding attack (NASRRF), and address spoofing based data flooding attack (ASRRF) [15]. In ASRRF, the attacker transmits a false route request packet by modifying the IP address, but in NASRRF, the attacker floods the network with a false route request packet and maintains the same IP address. In the case of NASDF, the attacker saturates the network by sending fake data packets alongwith identical IP addresses. In ASDF, on the other hand, the attacker overwhelms the network with fake data packets while changing the IP address.

Kennedy and Eberhart invented Particle Swarm Optimization (PSO) in 1995, a population-based global optimization methodology based on evolutionary computational intelligence [41]. It is based on the social behavior of birds flocking for food. PSO is a population-based search method.

C. *Amplification Attack*

The broadcast IP address functionalities are used to repeat and amplify a domain name system (DNS) amplification attack (as depicted in Figure 8).

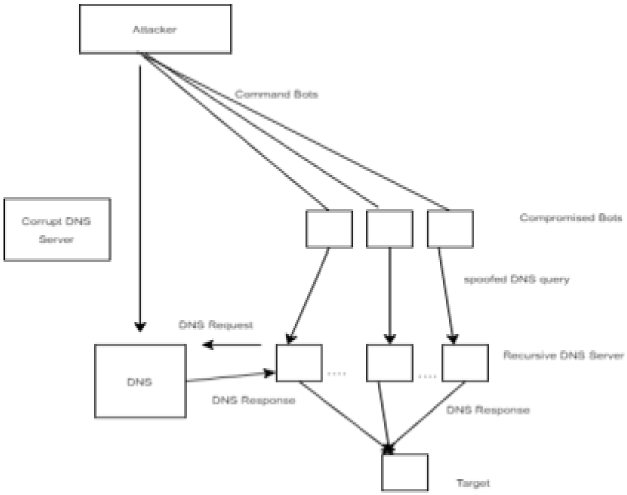

Fig 8 DNS Amplification Attack.

Instead of assigning a particular address as the destination, it allows a sender system to provide a broadcast IP address [26]. Consequently, packets are duplicated across the network and transmitted to each IP address. This type of DDoS attack amplifies the amount of assaulting traffic by either directly delivering the broadcast message or utilizing agents.The attacker does not have to sneak up on the devices of the broadcast network if they decide to transmit a broadcast message directly or without installing any agent software.

As a result, hackers can access sensitive data belonging to customers through application bugs, buffer overflows, and other vulnerabilities [10]. Zero day attacks cannot be stopped from the beginning, notwithstanding the fact that a data repository on the application layer has been established to fend off such attacks.

IV. LAYER BASED IoT ARCHITECTURE.

Architecture is a structure of network's specification, function,configuration,principles and procedures. Internet of Things comprises of huge number of smart devices connected to a broad network[17]. As there are various technologies involved in it and that too wireless manner. This makes the entire structure complexso we need an architecture to simplify the scenario.

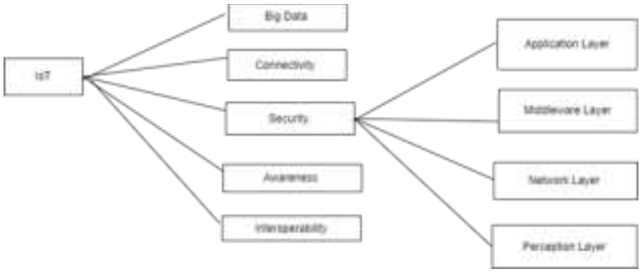

Fig. 8. Layer based IoT Architecture.

As evident from Figure 9 , There are four layers of IoT architecture:

The **Middleware** layer is in charge of analyzing data collected by sensor nodes. At this layer, computational as well as processing resources are required. The key difficulties in securing data in this tier are cloud and authentication. [11]. Because it is a newer domain compared to the network layer, threats and vulnerabilities must be investigated. [12]

The **Application** layer is the means via which data is made useful to the user. This layer is also known as the Process Layer [9]. In this case, the Attacker seeks illegal internet connection to the program. This allows attackers to gain access to the user's sensitive data via exploiting vulnerabilities, defects in applications, causing buffer overflows, and so on [10]. Notwithstanding the repository being designed at the application layer to protect against this kind of attack, zero-day attacks cannot be stopped.

Elements that are primarily wired or connected via wireless or possess both capabilities make up the Network Layer. Such nodes need a fundamental protocol layer for data transfer. In such a network, gateways may be present and function to collect data as well as transfer it across nodes.

In an Internet of Things setting, the **perception layer** is in charge of information transmission and sensing. A few of the tools used to extract and collect data are RFID tags, smart cards, and sensor nodes. Devices used at the Perception Layer are limited by the availability of resources when it comes to user utilization. Methods with limited data transfer range, such as RFID, NFC, Bluetooth, ZigBee, and many more, can also be misused.

A. Security solutions at various layers.

1) Application Layer

For identifying a DDoS attack on an application layer, one should become habituated with typical traffic patterns. The end users may become concerned whenever there is a deviation from the usual traffic pattern. Furthermore, it is nearly hard to extract signatures for zero-day assaults. In order to combat DoS attacks using string hits, Afek et al. [31] suggested using the DHH (Double Heavy Hitters) and THH (Triple Heavy Hitters) algorithms. An algorithmic test of this approach in a simulation showed that it is highly precise in detecting DoS attach. A method based on "Auto Encoder" was put out by Gurina et al. [32] to identify SQL Injection Attacks at the application layer. This technique provided minimal latency while extending high precision detection.

2) Middleware Layer

Tsai et al. [33] presented a user authentication system that may be implemented across several servers, regardless of their geographical locations. By implementing that, access control as well as authentication will be expanded to encompass not only servers, but also the final user. Employing a reliable third party for handling user authentication can prevent any delays in implementing this proposed solution. This will provide robust security measures to protect Middleware Layer cloud services from unauthorized access and effectively mitigate Distributed Denial of Service (DDoS) assaults. The proposed approach by Shafagh et al. [34] could help Middleware Layer servers in securely storing data in databases. The Encrypted Query Processing Approach, also referred to as EQPA, enables end users to perform queries on a database that has been encrypted. This approach employs algorithms with low complexity. The specifics have been demonstrated in Table 3.

TABLE III. CLASSIFICATION OF IoT ATTACKS AND THEIR COUNTERMEASURES.

Layers	Attacks	Countermeasures
Application	1.Buffer Overflow 2. Phishing 3.Reprogramming Attack 4. Code Injection	1, Risk Assessment 2.Data Security 3.Intrusion Detection 4.Firewalls
Middleware	1. Flooding 2. SQL Injection 3.Signature wrapping 4.Web browser	1, Web Application Scanners 2.Homomorphic Encryption 3.Fragmentation Redundancy

Network	1.Flooding 2.DoS 3,Man In the Middle 4. Replay Attack	1, Routing Protocols 2.Data Privacy 3.Authentication 4.Ad-hoc routing
Perception	1, RF Jamming 2.Bootstrap 3. Spoofing 4. Kill Command.	1. Secure Physical Design 2.Risk Assessment. 3.Device Authentication 4. Data Privacy

3) *Network Layer*

Authentication procedures were highlighted by Salman et al.[35] as a feature that could help to reduce IoT security risks. To address the diversity in the Internet of Things and integrate several protocols, researchers introduced an identity-based authentication approach that leverages software defined networking (SDN) for IoT devices. The effectiveness of these efforts was assessed by constructing a system that was investigated using the AVISPA tool. The findings revealed that the scheme is resilient against replay, man-in-the-middle, as well as masquerade attacks. The mutual authentication architecture developed by Santos et al.[36] enables devices with minimal resources to securely connect with one other over the internet utilizing datagram transport layer security (DTLS).Additionally, the author suggested a gadget known as the Internet of Things Security Support Provider (IoTSSP),is in charge of maintaining device certificates, offering authentication services, and starting device sessions.

4) *Perception Layer*

For IoT infrastructure, Salami et al. [37] suggested using lightweight encryption. This method was created especially for devices with limited resources, and its outstanding management features provided a benefit at the Perception Layer. Significant changes regarding the PKI-Lite security protocol were suggested by Li et al. [38] in order to address the security issues related to the Internet of Things. A lightweight authentication technique described by Porambage et al. [39] has been widely used. This method was created with the limited resources at the sensor's end in mind. Furthermore, in light of it, the essential establishment method was also improved. Secrecy boosting techniques have been studied by Lin Hu et al. [40] to reduce potential outages during eavesdropping attacks at the perception layer.

V. CONCLUSION AND FUTUREWORK

IoT devices have limitless potential for use and intelligence. Since the IoT market lacks standards, every link could weaken the network. The challenges leading to common IoT architecture is still unanswered. We emphasized the security as well as privacy issues in the IoT space in this research. We've also looked at the overall IoT architecture along with the security concerns at the different layers of the IoT protocol stack. The article also covers the criteria for security services in IoT and the main obstacles to IoT security. Additionally, we have included a succinct summary of the current methods for protecting IoT devices.

The paper also points out the following IoT security services: Confidentiality, Integrity as well as Authentication. There are numerous important features what IoT is capable of. Security has become a challenging issue for IoT.In our work, the comparison between various attacks operating on different IoT layers are discussed with some necessary countermeasures. We have highlighted a layer based architecture for simplifying the complicated IoT features arose due to wireless methodologies.

Due to the growing number of computer services, IoT has recently achieved significant appeal. However, one of the biggest IoT issues and the fundamental concern addressed by various Internet-of-things investors remains protection, as does the option to postpone its deployment. It is then concluded that a number of important issues ought to be addressed for the purpose to promote IoT in the real world. Security is a critical aspect of an IoT network, and it is tied to certain safety precautions that are also essential for a device to guarantee secrecy and security. IoT security is a branch of information security that concentrates on smart app security, information security, and particularly digital revolution networks.

REFERENCES

[1] H. F. Atlam, R. J. Walters, and G. B. Wills, "Internet of things: State-of-the-art, challenges, applications, and open issues," Int. J. Intell. Comput. Res., vol. 9, no. 3, pp. 928–938, 2018. DOI: https://doi.org/10.20533/ijicr.2042.4655.2018.0112

[2] Atlam, H.F., Walters, R.J., Wills, G.B.: Intelligence of Things: Opportunities & Challenges.3rd Cloudification of the Internet of Things (CIoT), pp. 1–6 (2018)

[3] P. Guillemin and P. Friess, Internet of things strategic research roadmap. Media, Luxembourg: Eur. Comm. Inf. Soc., 2009.

[4] ITU, Overview of the Internet of things. Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp.Next-generation networks - Fram. Funct. Archit. Model, 2012, p. 22.

[5] W. Stallings, "The internet of things: Network and security architecture," Internet Protocol J., vol. 18, no. 4, pp. 2–24, 2015.

[6] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, Developing an adaptive Riskbased access control model for the Internet of Things. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)and IEEE Cyber, Physical and Social Computing(CPSCom) and IEEE Smart Data(SmartData),no. June, pp. 655–661 (2017)

[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.https://doi.org/10.1016/j.future.2013.01.010

[8] J. M. Batalla, G. Mastorakis, C. X. Mavromoustakis, and E. Pallis, Beyond the Internet of Things. Switzerland: Springer, 2017. DOI: https://doi.org/10.1007/978-3-319-50758-3

[9] S. Al Hinai and A. V. Singh, (2017, December). Internet of things: Architecture, security challenges and solutions. In 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS) (pp. 1-4). IEEE.

[10] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, et al., "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," J. Hardw. Syst. Secur., vol. 2, no. 2, pp. 97–110, 2018.https://doi.org/10.1007/s41635-017-0029-7

[11] S. Deep, X. Zheng, and L. Hamey, (2019). A survey of security and privacy issues in the Internet of Things from the layered context.arXiv preprint arXiv:

[12] I. Cvitić, M. Vujić, and S. Husnjak, (2016, January). Classification of security risks in the IoT environment. In 26th Daaam International Symposium on Intelligent Manufacturing and Automation (pp. 0731-0740).

[13] M. Daud, R. Rasiah, M. George, D. Asirvatham, A. F. A. Rahman, and A. Ab Halim, (2018, May). Denial of service:(DoS) Impact on sensors. In 2018 4th International Conference on Information Management (ICIM) (pp. 270-274). IEEE.

[14] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, vol. 47, no. 6, pp. 53–57, 2004.https://doi.org/10.1145/990680.990707

[15] S. Gurung and S. Chauhan, "A novel approach for mitigating route request flooding attack in MANET," Wirel. Netw., vol. 24, no. 8, pp. 2899–2914, 2018., https://doi.org/10.1007/s11276-017-1515-0

[16] W. Yin, P. Hu, J. Wen, and H. Zhou, ACK spoofing on MAC-layer rate control: Attacks and defenses,Computer Networks,Volume 171,2020,107133,ISSN 13891286,https://doi.org/10.1016/j.comnet.2020.107133

[17] A. Roohi, M. Adeel, and M. A. Shah, "DDoS in IoT: A Roadmap Towards Security & Countermeasures," 2019 25th International Conference on Automation and Computing (ICAC), 2019, pp. 1-6, DOI: https://doi.org/10.23919/IConAC.2019.8895034

[18] D. Puthal, R. Ranjan, and J. Chen, "Big Data Stream Security Classification for IoT Applications," in Encyclopedia of Big Data Technologies, S. Sakr and A. Y. Zomaya, Eds. Cham: Springer, 2019, https://doi.org/10.1007/978-3-319-77525-8_236

[19] Sunil Kumar Jangir and Naveen Hemrajani, 2016. Evaluation of Black hole, Wormhole and Sybil Attacks in Mobile Ad-hoc Networks. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '16). Association for Computing Machinery, New York, NY, USA, Article 74,16. https://doi.org/10.1145/2905055.2905133

[20] E. Fazeldehkordi, I. S. Amiri, and O. A. Akanbi, Chapter 4 - Investigation and Selection Procedure,Editor(s): Elahe Fazeldehkordi, Iraj Sadegh Amiri, Oluwatobi Ayodeji Akanbi,A Study of Black Hole Attack Solutions,Syngress,2016,Pages 65-82,ISBN 9780128053676,

https://doi.org/10.1016/B978-0-12-805367-6.00004-1

[21] M. Kaur and A. Singh, "Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network," 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), 2016, pp. 217-221, DOI: 10.1109/ICMETE.2016.117.

[22] S. Banga, H. Arora, S. Sankhla, G. Sharma, and B. Jain, (2021) Performance Analysis of Hello Flood Attack in WSN. In: Purohit S., Singh Jat D., Poonia R., Kumar S., Hiranwal S. (eds) Proceedings of International Conference on Communication and Computational Technologies. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-5077-5_30

[23] S. Specht and R. Lee, Taxonomies of distributed denial of service networks, attacks, tools and countermeasures. Princeton, NJ, USA: Princeton University, 2003, pp. CEL2003–CEL03.

[24] Singh, K. J., & De, T. (2017). Analysis of application layer DDoS attack detection parameters using statistical classifiers. Internetworking Indonesia, 9(2), 23-31. 4, 971–1001.

[25] K. Johnson Singh, K. Thongam, and T. De, "Entropy-based application layer DDoS attack detection using artificial neural networks," Entropy (Basel), vol. 18, no. 10, p. 350, 2016. https://doi.org/10.3390/e18100350

[26] I. L. Meitei, K. J. Singh, and T. De, (2016, August). Detection of DDoS DNS amplification attack using classification algorithm. In Proceedings of the International Conference on Informatics and Analytics (pp. 1-6) https://doi.org/10.1145/2980258.2980431

[27] N. Anand and K. J. Singh, "An Overview on Security and Privacy Concerns in IoT-Based Smart Environments," in Security, Privacy and Data Analytics. ISPDA 2022. Lecture Notes in Electrical Engineering, vol. 1049. U. P. Rao, M. Alazab, B. N. Gohil, and P. R. Chelliah, Eds. Singapore: Springer, 2023, https://doi.org/10.1007/978-981-99-3569-7_21

[28] N. Michael, "Benchmark Harness," in Encyclopedia of Big Data Technologies, S. Sakr and A. Y. Zomaya, Eds. Cham: Springer, 2019, https://doi.org/10.1007/978-3-319-77525-8_134

[29] N. Anand and K. J. Singh, "A Comprehensive Study of DDoS Attack on Internet of Things Network," in Recent Advances in Electrical and Electronic Engineering. ICSTE 2023. Lecture Notes in Electrical Engineering, vol. 1071. B. P. Swain and U. S. Dixit, Eds. Singapore: Springer, 2024, https://doi.org/10.1007/978-981-99-4713-3_56

[30] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecomm. Syst., vol. 73, no. 1, pp. 3–25, 2020.https://doi.org/10.1007/s11235-019-00599-z

[31] Y. Afek, A. Bremler-Barr, and S. L. Feibish, "Zero-Day Signature Extraction for High-Volume Attacks," IEEE/ACM Trans. Netw., vol. 27, no. 2, pp. 691–706, 2019. https://doi.org/10.1109/TNET.2019.2899124

[32] A. Gurina and V. Eliseev, "Anomaly-Based Method for Detecting Multiple Classes of Network Attacks," Information (Basel), vol. 10, no. 3, p. 84, 2019. https://doi.org/10.3390/info10030084

[33] J. L. Tsai and N. W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," IEEE Syst. J., vol. 9, no. 3, pp. 805–815, 2015. https://doi.org/10.1109/JSYST.2014.2322973

[34] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, (2015, September). Poster: Towards encrypted query processing for the Internet of Things. In Proceedings of the 21st annual international conference on mobile computing and networking (pp. 251-253). ACM. https://doi.org/10.1145/2789168.2795172

[35] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, Identity-based authentication scheme for the internet of things. Paper presented at: Proceedings of the 2016 IEEE Symposium on Computers and Communication (ISCC); 2016:1109-1111; IEEE. 68. Santos DOI: https://doi.org/10.1109/ISCC.2016.7543884

[36] G L, Guimaraes V T, Cunha R G, Granville LZ, Tarouco LM R. A DTLS-based security architecture for the Internet of Things. Paper presented at: Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC); 2015:809-815; IEEE.

[37] S. Al Salami, J. Baek, K. Salah, and E. Damiani, (2016, August). Lightweight encryption for smart home. In 2016 11th International Conference on Availability, Reliability and Security (ARES) (pp. 382-388). IEEE. https://doi.org/10.1109/ARES.2016.40

[38] Z. Li, X. Yin, Z. Geng, H. Zhang, P. Li, Y. Sun, et al., (2013, January). Research on PKI-like Protocol for the Internet of Things. In 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation (pp. 915-918). IEEE.

[39] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," Int. J. Distrib. Sens. Netw., vol. 10, no. 7, p. 357430, 2014. https://doi.org/10.1155/2014/357430

[40] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, et al., "Cooperative jamming for physical layer security enhancement in internet of things," IEEE Internet Things J., vol. 5, no. 1, pp. 219–228, 2018. https://doi.org/10.1109/JIOT.2017.2778185

[41]S. Agarwal, A. P. Singh and N. Anand, "Evaluation performance study of Firefly algorithm, particle swarm optimization and artificial bee colony algorithm for non-linear mathematical optimization functions," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 2013, pp. 1-8, https://doi.org/10.1109/ICCCNT.2013.6726474