Palak Patel[1]
Dr. Chintan Shah[2]
Dr. Premal Patel[3]

A Comprehensive Review of IoT Security: Challenges, Authentication Mechanisms

Abstract
The integration of IoT, blockchain, cloud computing, and encryption is transforming healthcare systems by addressing key challenges in security, privacy, and data management. This study examines innovative authentication frameworks for securing electronic health records (EHRs) and healthcare management systems, emphasizing the role of blockchain in enhancing data integrity, decentralization, and secure data sharing. Blockchain prevents single points of failure and ensures patient privacy through encryption and pseudonymization. Authentication mechanisms like multi-factor authentication (MFA), smart cards, and biometrics are crucial for mitigating threats such as replay attacks, man-in-the-middle attacks, and unauthorized access. For IoT-enabled healthcare, securing communication between devices and servers is essential. Techniques like Elliptic Curve Cryptography (ECC), fuzzy extractors, and Physically Unclonable Functions (PUFs) provide efficient, secure communication while minimizing computational burden. The study proposes an advanced security model that integrates lightweight encryption to address challenges in scalability, heterogeneity, and cyber threats. It also includes dynamic key-based authentication and context-aware authentication using RSSI to enhance security. This model ensures robust security for IoT-enabled healthcare systems, addressing emerging risks and ensuring the resilience of healthcare infrastructures. The research aims to optimize resource utilization, mitigate sophisticated cyber threats, and provide cost-effective scalability for secure, efficient health data management.

Keywords: Internet of Things (IoT), Blockchain, Cloud Computing, Electronic Health Records (EHRs), Authentication, Security, Privacy, Elliptic Curve Cryptography (ECC), Physically Unclonable Functions (PUFs), Data Integrity

INTRODUCTION

Since the Internet of Things (IoT) was introduced in 1999, its meaning has continuously evolved. The notion of IoT originated from the domain of RFID (Radio Frequency Identification). The Internet of Things (IoT) enables intelligent recognition, placement, and monitoring of objects by affixing electronic labels to each item. Nevertheless, the evolution of IoT rapidly transcends this limited definition and expands into conventional IT domains. The meaning of IoT has been consistently enhanced. Some individuals anticipate that the Internet of Things will represent history's third wave of information technology a term that refers to a significant shift in how we interact with and use technology, similar to the advent of the internet and the proliferation of personal computers. Following an extensive examination of several definitions of IoT, the Internet of Things may be roughly characterized as follows: Data is current as of October 2023.2[3] Equipping individuals, objects, transactions, or processes with the capability to sense, transmit, and process information through the utilization of sensing devices [2]. IoT is now being applied in many fields like healthcare, agriculture, transportation, smart cities, etc. In contrast, its widespread use has introduced substantial vulnerabilities due to IoT devices often functioning in resource-constrained scenarios, where they possess reduced computational capabilities and memory. In this paper focus on traditional security measures infeasible, exposing IoT systems to various threats including replay attacks, man-in-the-middle attacks, device spoofing, and denial-of-service attacks. To overcome these issues, it is vital to implement lightweight authentication protocols which are capable of guaranteeing strong security in a cost-effective manner. Using the power of advanced cryptographic techniques like Elliptic Curve Cryptography (ECC) as well as context-aware specifications like Received Signal Strength Indicator (RSSI), lightweight authentication approaches can harden IoT environments against the new vulnerabilities and attacks while providing secure communication and keeping sensitive information safe across ubiquitous networks [4]. Cryptography and authentication, securing IoT-enabled healthcare systems is especially critical. In healthcare, IoT devices are used to monitor patient conditions, collect health data, and enable telemedicine, making it essential to protect sensitive patient data from unauthorized access and tampering. Therefore, healthcare IoT systems need advanced encryption techniques to ensure data confidentiality, integrity, and authenticity. The integration of lightweight encryption schemes with ECC and context-aware authentication methods provides a strong defense against common security threats while also being efficient enough to run on the limited resources of IoT devices [5]. These techniques ensure that healthcare organizations can exchange sensitive data securely across devices and cloud platforms, mitigating risks associated with data breaches and unauthorized access. The adoption of IoT in industries such as smart cities, healthcare, and industrial automation has introduced significant advancements in operational capabilities. However, the increase in connected devices also means more potential entry points for cybercriminals. Therefore, the IoT ecosystem must evolve to address not only the technological challenges of secure data transmission but also the strategic challenge of scaling security solutions as the number of connected devices grows. Hybrid solutions that combine software and hardware security measures offer an effective way to safeguard IoT devices and networks [6]. Recent research has also focused on optimizing resource utilization, ensuring that security protocols do not drain resources while still providing robust protection. In sectors like healthcare, where sensitive patient data is transmitted over IoT networks, ensuring data integrity and privacy is paramount. Lightweight authentication protocols,

[1,2,3]Aditya Silver oak Institute of Technology, Silveroak University, Ahmedabad, Palakpatel.rs@silveroakuni.ac.in[1]

such as those utilizing ECC and RSSI, help mitigate risks and ensure secure data transmission in a cost-effective manner. With the continuous growth of IoT, there is a critical need for scalable, robust security solutions that can handle the increasing complexity of IoT networks without compromising device performance. These advancements in authentication protocols offer a pathway to a secure and resilient IoT ecosystem, capable of safeguarding personal data and maintaining the integrity of communication networks while supporting the wide-scale adoption of IoT technologies.

IoT ARCHITECTURE

A. Three Layers of IoT

In IoT Architecture consider mainly 3 layers as main Layers in IoT: Namely Application Layer, Network Layer, Perception Layer.

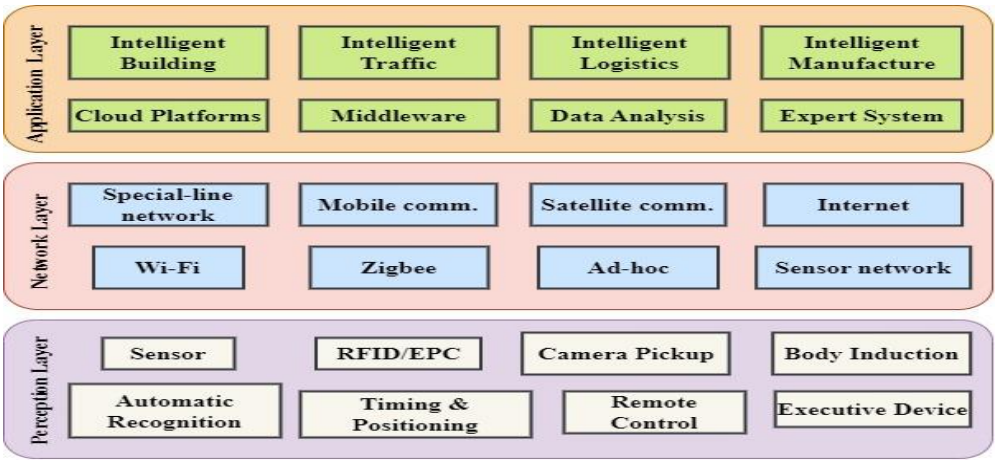

Figure 1: Three Layers Architecture of IoT [7]

(1) Perception Layer: It is the lowest layer in the three-layer architecture of IOT, which may also be called the perception and control layer. Perception layer essential completes collection of data of person, physical object, transaction or process etc. with use of specific perception tools. Perceptual tools with different types; general involving general application of the IOT, such as a variety of sensors, transmitters (gas concentration sensor, temperature sensor, humidity sensor, current transformer, voltage transducer, etc.), RFID tag/EPC code scanner, timing and positioning terminal (GPS or CELL), webcam/microphone, human body infrared sensor, remote measuring and controlling device, as well as automatic identification equipment and so on. Perception layer involves the aggregate effect stage that builds the final step of the information processing and packaging when the stage of information collection is over. The executive devices provide the control operations as per requirement by taking control information from coming network layer [7].

(2) Network Layer: The upper layer of three-layer architecture it could also be called the transmission layer. The Network layer deliver the stream of data that the perception layer collects to the application layer in a secure, rapid and reliable manner, realizing communication exchange between perception layer and application layer through various networks. It is advisable to mention that data communication capability of network layer involves both short distance transmission and distant data communication. This communication or sensor network, used in close range transmission, can be a wired or wireless, like Wi-Fi, Ad-hoc, Mesh, Zigbee, industrial bus, etc [7].

(3) The Application Layer: the three layers architecture top even level. Application layer: it is the layer to analyze and deal with the information coming from the perception layer and the network layer, realize the IOT application. The application layer can be regarded as the interface between the IOT and all kinds of users (some human, some system) and with specific needs, to realize various intelligent applications of IOT. Such as intelligent building, intelligent traffic, intelligent logistics, intelligent manufacturing, vehicle navigation and security monitoring. The intelligent applications of IOT still depend on IT support, such as cloud computing technology, database technology, data mining technology, middleware technology, multimedia technology, expert systems, etc [7].

Security in IoT

Despite such giant importance and enormous applications of IoT, deploying it in mission critical application areas, where security and privacy is major of most important concerns, is not simple. For instance, a malicious attack on smart healthcare system can lead to the death of many patients which is a great concern, likewise it can also lead to financial and human loss in case of intelligent transportation system. IoT Security is a quite problematic region which need more research work in order to handle with these hardships. We take about these security challenges.

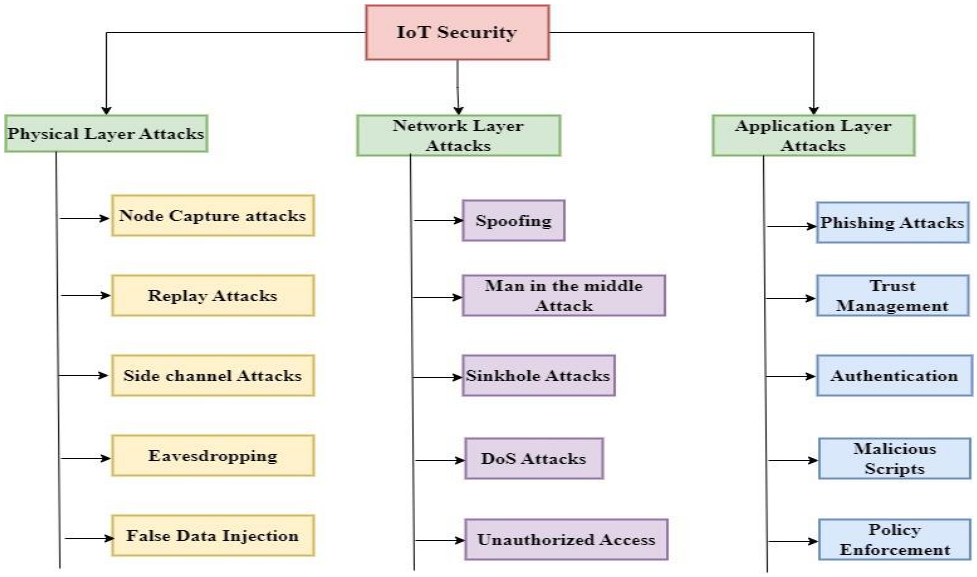

Figure 2: IoT Security and Attacks Layer-wise [29]

IoT Security: Layer-wise Attacks

1. Physical Layer Attacks

The physical layer in IoT systems is responsible for sensing, transmitting, and receiving data from physical objects. It is highly vulnerable due to the physical accessibility of devices, making it prone to the following attacks:

- **Node Capture Attacks**: Attackers physically access and compromise IoT nodes to extract sensitive data, such as cryptographic keys, or reprogram the device to act maliciously.
- **Replay Attacks**: Attackers intercept and retransmit data packets to deceive the system, making it believe that an action occurred multiple times or is still valid.
- **Side Channel Attacks**: These involve analyzing the physical properties of a device (e.g., power consumption, timing, or electromagnetic emissions) to gain unauthorized access to sensitive data.
- **Eavesdropping**: An attacker passively intercepts communication between IoT devices to gather confidential information without altering the data.
- **False Data Injection**: Malicious data is introduced into the network, leading to incorrect decisions or operations in IoT systems.

2. Network Layer Attacks

The network layer facilitates communication between IoT devices and servers, making it susceptible to various attacks targeting data transmission. Key network layer attacks include:

- **Spoofing**: Attackers impersonate a legitimate device or user by falsifying their identity, allowing unauthorized access to the network.
- **Man-in-the-Middle (MITM) Attack**: The attacker intercepts and manipulates data between two communicating devices without their knowledge, potentially altering or stealing the data.
- **Sinkhole Attacks**: An attacker creates a malicious node within the network that attracts traffic from other nodes, disrupting data routing and causing packet loss.
- **DoS (Denial of Service) Attacks**: Attackers flood the network with excessive traffic, overwhelming its resources and causing service disruptions.
- **Unauthorized Access**: Intruders exploit vulnerabilities to gain unauthorized control over network resources, leading to data breaches or malicious activity.

3. Application Layer Attacks

The application layer is where IoT services and functionalities are delivered to end-users. It is a critical layer that is often targeted by attackers aiming to compromise services. Common application layer attacks include:

- **Phishing Attacks**: Attackers trick users into divulging sensitive information, such as login credentials, by creating fake websites or messages resembling legitimate services.
- **Trust Management Attacks**: These exploit weak trust relationships within IoT networks, manipulating trust scores or policies to gain unauthorized access.
- **Authentication Attacks**: Attackers bypass or compromise authentication mechanisms to access restricted areas or data. Weak authentication processes often exacerbate this issue.
- **Malicious Scripts**: Injecting malicious code into IoT applications to compromise their functionality, steal data, or disrupt operations.
- **Policy Enforcement Attacks**: These target the enforcement of security policies within IoT systems, bypassing or disabling policies to gain unauthorized access or control.

LITERATURE REVIEW

Sr. No	Types of Attack	Solution
1	DOS	Denial-of-service attacks constitute a major security risk to IoT devices. Intelligent devices used for real-time monitoring had service availability as a key parameter. IoT mobile technology applications require reliable and efficient data transmission, with successful data delivery to the node. In order to avoid the false behavior of the user or address deviations from the end-to-end communication, many lightweight authentication communication methods have been incepted [10][11][12].
2	MITM	Intermediate devices like switches and controllers are used to network and implement smart devices in various applications. In addition to that, most intelligent devices are hooked up using wireless communication protocols. The Bloom lightweight countermeasure is activated upon the compromise of devices within the owner network or when an attacker gains information through an unsecured channel, thus utilizing the protocol based on Bloom filters to monitor the packets of changes and detect certain types of MITM attacks [14].
3	Routing attacks	smart devices may communicate in a decentralized, centralized, or dynamic way. In IoT networks, network-level security is a challenge as traditional encryption methods are associated with increased energy consumption. Taking a systematic approach, tackling this problem head-on with a slim machine-learning methodology. If effective, this technique can enhance the security of IoT applications to a high level for a secure and efficient IoT ecosystem [15] [16] [17].
4	Malicious attacks	Malicious code is unknown software designed to obtain passwords or data that can harm the device. However, it is important to note that due to the resource constraints, the IoT devices are prone to malicious attacks. Diverse methodologies are important for detecting rogue nodes to maintain the system security integrity. While traditional security solutions can be effective in certain cases, they often do not fully meet the unique challenges presented by IoT devices. Use proposed approach like multi-layer game protocol and privacy-preserving game-based strategy [18]-[25].
5	Trust Management	The recognition and mitigation of hazardous threats are done in safe ways, thereby increasing the confidence of the user group. In Internet of Things applications, trust management is a key challenge, which the secure platform based on blockchain technology solves [26]-[28].

Table 1: Types of Attacks and it's solution

Layer	Examples	Security Challenges	Proposed Solution
Application Layer	Smart Health Smart Industries Smart Homes Smart Transportation	Privacy Violation/Insecure Interfaces -Privacy violation/Insecure Firmware -Privacy /Middleware Security	-Verification of Password Strengths, Secure coding (SQL injection) using HTTPS & firewalls - Authentication in secure Communication, key management, lightweight encryption systems
Support Layer	Smart Computing Fog & Cloud Computing	Privacy Violation/ End to End Security Denial-of-service	- Using secure cloud computing techniques, applying advanced and lightweight encryption system AES, SHA (Cipher based). - Authentication based on Long Asymmetric Key.
Network Layer	Mobile Network Internet/IPV6 Wireless Network	- Replay or duplication attacks - Insecure Neighbour Discovery -Eavesdropping/ Routing Attack -sinkhole & wormhole attacks - Privacy violation/authentication & Secure Communication	- Introducing timestamp and nonce options for verification and defining checksum by hash value -Encryption (ECC)based signatures for authentication -Light weight Authentication system for Authentication. - anomaly detection, signal strength management -lightweight ticket granting system, symmetric and asymmetric encryption algorithms
Perception Layer	Sensors Gateways RFID Readers	- Jamming -spoofing attacks -Insecure initialization & Configuration	- Measure signal strength, compute packet delivery ratio -channel estimation, signal strength -Add Artificial Noise and data transmission rate between Node.

Table 2: Layer wise attack and It's Solution

Research Gap

Authentication methods for Electronic Health Records (EHR) Systems rely on a single-key or password-based authentication for an entity existing in the network. These are simple but weak implementations and are susceptible to many attack vectors, such as key duplication, side-channel attacks, man-in-the-middle (MITM) attacks, device cloning, dictionary attacks, etc. Keying material is repeated, which leads to a significant drawback in these works, i.e., static keys or passwords being unchanged during the whole lifetime of the network. This practice drastically raises the chances of a compromise, as the adversary can use dictionary attacks to break static passwords or physically collect shared keys used between the devices and replicate them with cloned devices, which will return the obtained responses to the system, leading to the system's security and integrity being weakened.

This revaluation highlights another important gap in the key management mechanisms. In the absence of periodic key updates or rotation, the adversary's access over time cannot be limited as there is also no built-in mechanism to limit it in case of key compromise. Thus, there is an urgent demand for an authentication scheme that employs the method of dynamic key update to adversaries with a shared key to protect the system from being accessed by other users. In addition, existing approaches often do not provide mutual authentication, which is necessary to ensure the server identity and the identities of participant entities, including sensor nodes and users. Without mutual authentication, the system is susceptible to impersonation attacks and can undermine trust across the network.

To combat these gaps, we need to establish a strong two-party authentication design system with a dynamic key mechanism to counter various attacks, such as MITM, interception, dictionary, key theft, and cloning and replay attacks. Such an approach would vastly improve electronic healthcare records systems' security posture and reliability, protecting sensitive healthcare data and reducing the vulnerabilities to adversarial actions.

Proposed System

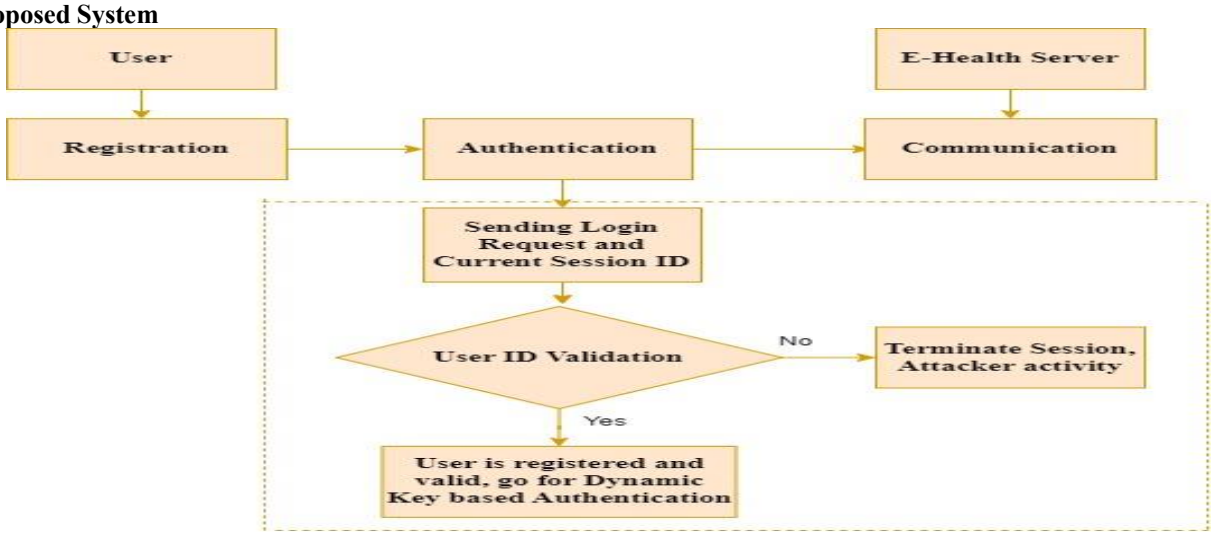

Figure 3: Proposed System

User

The process starts with the user, who interacts with the e-health system to gain access to their health records or perform other healthcare-related activities. The user must first go through a registration process to create a valid account in the system before being authenticated.

Registration

The registration phase is where the user provides their details, which are securely stored in the E-Health Server. This step ensures that only legitimate users are allowed into the system. It also involves creating unique credentials, such as a username and password, or biometric authentication data, which will be used in future login attempts. This data is typically encrypted to prevent unauthorized access.

Authentication

After registration, when a user attempts to log in, they go through the authentication phase. This phase ensures that the user is who they claim to be before allowing access to the healthcare system. The authentication step includes sending a login request along with a session ID, which is a temporary token generated for secure login sessions.

Sending Login Request and Current Session ID

When a user initiates a login, their credentials (such as username and password) are sent to the E-Health Server for verification. A session ID is generated dynamically, which helps in preventing replay attacks and other security breaches. The session ID ensures that each authentication attempt is unique and not reused by an attacker.

User ID Validation
The User ID Validation step determines whether the user's credentials match the records stored in the E-Health Server. If the user is not recognized, the authentication request is denied, and the session is terminated to prevent any unauthorized access. If the validation is successful, the user proceeds to the next authentication step.

Terminate Session, Attacker Activity
If the User ID Validation fails, the system considers the login attempt as a possible attacker activity and immediately terminates the session. This prevents attackers from making repeated login attempts using stolen or guessed credentials. The session termination also blocks further communication from the unauthorized user, ensuring system security.

User is Registered and Valid, Go for Dynamic Key-Based Authentication
If the User ID Validation is successful, the system proceeds with Dynamic Key-Based Authentication. This involves generating a one-time dynamic authentication key for secure access. The dynamic key is more secure than static passwords, as it changes for every session, making it difficult for attackers to reuse credentials or perform man-in-the-middle attacks.

E-Health Server
The E-Health Server is responsible for storing and managing patient records, authenticating users, and handling communication between users and the healthcare system. It verifies credentials, generates session IDs, and ensures that only authenticated users can access sensitive health data.

Communication
Once authentication is completed successfully, the user is granted secure access to the E-Health Server, allowing them to retrieve or manage their health records. The communication channel between the user and the server is encrypted, ensuring data privacy and security.

CONCLUSION

The Internet of Things (IoT) has revolutionized various industries by enabling interconnected devices to communicate and share data seamlessly. While IoT offers immense opportunities in fields like healthcare, agriculture, transportation, and smart cities, its widespread adoption has introduced significant security challenges across all layers of its architecture. The perception layer is vulnerable to physical attacks like node capture, side-channel, and replay attacks, while the network layer faces threats such as spoofing, MITM, and DoS attacks. The application layer is prone to phishing, authentication bypass, and policy enforcement attacks. This study emphasizes the critical need for robust security measures tailored to IoT's unique architecture and constraints. Existing methods, such as static password- or key-based authentication, are insufficient as they are highly susceptible to attacks like key theft, dictionary attacks, and device cloning. The research highlights the need for lightweight, dynamic authentication mechanisms that can mitigate these risks effectively. Incorporating techniques like Elliptic Curve Cryptography (ECC), dynamic key updates, and mutual authentication is crucial to enhancing IoT security while addressing resource limitations. Future IoT security systems must focus on multi-layered, adaptive approaches that combine cryptographic techniques with context-aware methods like RSSI to protect sensitive data and ensure secure communication. Addressing the identified research gaps through innovative designs will safeguard IoT systems against evolving threats and maintain their integrity and reliability in mission-critical applications like healthcare, smart cities, and industrial automation. By closing these gaps, the IoT ecosystem can continue to grow while ensuring privacy, security, and trust among its users.

Futurework
To validate the security and effectiveness of the proposed authentication model, we plan to implement and test it using Automated Validation of Internet Security Protocols and Applications (AVISPA) and Security Protocol ANimator (SPAN). AVISPA is a well-established security verification tool used for analyzing cryptographic protocols to detect vulnerabilities such as man-in-the-middle attacks, replay attacks, and unauthorized access attempts. By modelling our dynamic key-based authentication system in AVISPA, we can rigorously evaluate its resilience against potential threats in an IoT-enabled healthcare environment.

REFERENCE

[1] Wei Emma Zhang, Quan Z. Sheng et al. "The 10 Research Topics in the Internet of Things" *published in 2nd IEEE International conference on RTEICT, 2020*
[2] Amit Kumar Tyagi and Ajith Abraham "Internet of Things: Future Challenging Issues and Possible Research Directions*" published in International Journal of Computer Information Systems and Industrial Management Applications, Vol. 12, pp. 113-124, 2020.*
[3] H. Shin, H. K. Lee, H. Cha, S. W. Heo and H. Kim, "IoT Security Issues and Light Weight Block Cipher," 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2019, pp. 381-384, doi: 10.1109/ICAIIC.2019.8669029.

[4] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
[5] Rekha, Shashi & Lingala, Thirupathi & Renikunta, Srikanth & Gangula, Rekha. (2021). Study of security issues and solutions in Internet of Things (IoT). Materials Today: Proceedings. 10.1016/j.matpr.2021.07.295.
[6] Jyoti Neeli, Shamshekhar Patil "Insight to security paradigm , research trend & statistics in internet of things(IoT)" Global Transitions Proceedings, Volume 2, Issue 1, 2021, Pages 84-90, https://doi.org/10.1016/j.gltp.2021.01.012.
[7] C. -l. Zhong, Z. Zhu and R. -G. Huang, "Study on the IOT Architecture and Access Technology," 2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES), 2017, pp. 113-116, doi: 10.1109/DCABES.2017.32.
8] Vangelis Gazis, Manuel Goertz Liang et al. "IoT Challenges, Projects, Architectures" *presented at IEEE 18th International Conference on Intelligence in next generation networks , 2015.*
[9] Jean Pierre Nzabahimana "Analysis of Security and Privacy Challenges in Internet of Things" *presented at IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018*
[10] M. Ghahramani, R. Javidan, M. Shojafar, R. Taheri, M. Alazab, and R. Tafazolli, "Rss: An energy-efficient approach for securing iot service protocols against the dos attack," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3619–3635, 2021.
[11] M. Stute, P. Agarwal, A. Kumar, A. Asadi, and M. Hollick, "Lidor: A lightweight dos-resilient communication protocol for safety-critical iot systems," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6802–6816, 2020.
[12] C. Lyu, X. Zhang, Z. Liu, and C.-H. Chi, "Selective authentication based geographic opportunistic routing in wireless sensor networks for internet of things against dos attacks," IEEE Access, vol. 7, pp. 31068–31082, 2019.
[13] C. Pu, "Sybil attack in rpl-based internet of things: Analysis and defenses," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4937 4949, 2020.
[14] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing sdn infrastructure of iot–fog networks from mitm attacks," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1156–1164, 2017.
[15] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in rpl-based iot environment using random forest rftrust," Computer Networks, vol. 198, p. 108413, 2021.
[16] N. Pavlovi´ c, M. ˇ Sarac, S. Adamovi´c, M. Saraˇcevi´c, K. Ahmad, N. Maˇcek, and D. K. Sharma, "An approach to adding simple interface as security gateway architecture for iot device," Multimedia Tools and Applications, pp. 1–16, 2021.
[17] B. Maram, J. Gnanasekar, G. Manogaran, and M. Balaanand, "Intelligent security algorithm for unicode data privacy and security in iot," Service Oriented Computing and Applications, vol. 13, no. 1, pp. 3–15, 2019.
[18] M. Hossain and J. Xie, "Third eye: Context-aware detection for hidden terminal emulation attacks in cognitive radio-enabled iot networks," IEEE Transactions on Cognitive Communications and Networking, vol. 6, no. 1, pp. 214–228, 2020.
[19] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, and Q. Cao, "Multistage signaling game-based optimal detection strategies for suppressing mal ware diffusion in fog-cloud-based iot networks," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1043–1054, 2018.
[20] M. R. Dey, U. Satapathy, P. Bhanse, B. K. Mohanta, and D. Jena, "Magtrack: Detecting road surface condition using smartphone sensors and machine learning," in TENCON 2019- 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 2485–2489.
[21] Z. Liu and Y. Wu, "An index-based provenance compression scheme for identifying malicious nodes in multihop iot network," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4061–4071, 2020.
[22] A. Agiollo, M. Conti, P. Kaliyar, T.-N. Lin, and L. Pajola, "Detonar: Detection of routing attacks in rpl-based iot," IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1178–1190, 2021.
[23] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," IEEE Access, vol. 8, pp. 199618 199628, 2020.
[24] C. Marche and M. Nitti, "Trust-related attacks and their detection: A trust management model for the social iot," IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3297–3308, 2021.
[25] A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," IEEE Transactions on Sustainable Computing, vol. 4, no. 1, pp. 88–95, 2019.
[26] M. D. Alshehri and F. K. Hussain, "A fuzzy security protocol for trust management in the internet of things (fuzzy-iot)," Computing, vol. 101, no. 7, pp. 791–818, 2019.
[27] S. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-based security management of iot infrastructure with ethereum transactions," Iran Journal of Computer Science, vol. 2, no. 3, pp. 189–195, 2019.
[28] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," IEEE Access, vol. 7, pp. 38947–38956, 2019.
[29] G. Savithri, B. K. Mohanta, and M. K. Dehury, "A Brief Overview on Security Challenges and Protocols in Internet of Things Application," *2022 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2022, pp. 1–6.