AI Based Reliable and Secure Data Transfer in Wireless Networks

P. Kalyanchakravarthi[1,2(✉)] and Susmitha Das[3]

[1] NIT Rourkela, Rourkela, India
kalyanecebujji@gmail.com
[2] Department of ECE, GMR Instiute of Technology, NIT Rourkela, Rajam, India
[3] Department of Electrical Engineering, NIT Rourkela, Rourkela, India
sdas@nitrkl.ac.in

Abstract. The rapid increase in digital data information is primarily driven by several interconnected factors like technological advancements, internet and connectivity, social media and online activities and Sensor Technologies, e-commerce and Online Transactions etc. The combination of advancing technology, widespread internet connectivity, the increasing adoption of digital devices and applications, and the demand for data-driven insights has led to an exponential increase in digital data information day by day. As technology continues to evolve, it is likely that this trend will continue for the foreseeable future. However, such rich sources of information are mostly left untapped. Authentication is essential in data transmission for several reasons. It plays a vital role in ensuring the confidentiality, integrity, and authenticity of data during transmission, helping to build trust in digital communications and safeguard sensitive information from unauthorized access or manipulation. This paper compares various methods available for data authentication and optimizes the solution with the help of Artificial Intelligence (AI). It can significantly enhance data authentication by providing advanced techniques and technologies to verify the integrity and authenticity of data. By leveraging AI's capabilities, organizations can strengthen their data authentication processes, reduce the risk of data breaches or fraud, and enhance overall data security. However, it's important to note that AI-based authentication systems are not infallible and should be used in conjunction with other security measures to provide robust protection against threats.

Keywords: Authentication Technology · Internet of Things. Security · Wireless Networks

1 Introduction

A wireless network refers to a communication system that enables the transfer of data between devices without the need for physical connections or cables. It utilizes wireless signals, typically in the form of radio waves, to transmit and receive information between devices such as computers, smartphones, tablets, IoT devices, and other network-enabled

X. Cheng (Ed): BROADNETS 2024, LNICST 601, pp. 320–328, 2025.
https://doi.org/10.1007/978-3-031-81168-5_30

devices. In a wireless network, devices communicate with each other through wireless access points or routers that facilitate the transmission of data [1]. These access points connect to a wired network infrastructure, such as a modem or Ethernet connection, which in turn connects to the internet or other networks.

Wireless networks can operate using different wireless communication protocols, such as Wi-Fi (Wireless Fidelity), Bluetooth, cellular networks (like 3G, 4G, and 5G), satellite communication, and others. Wi-Fi is one of the most commonly used wireless technologies for local area networking, providing wireless internet connectivity in homes, offices, public spaces, and various other environments.The wireless network infrastructure consists of devices such as routers, wireless access points, wireless adapters, and antennas that transmit and receive signals [2]. These devices employ wireless standards and encryption methods to ensure secure and reliable data transmission.

Wireless networks have revolutionized the way we connect, communicate, and access information. They offer benefits such as mobility, flexibility, and ease of use, enabling users to access the internet and network resources from anywhere within the network's coverage area [3]. There are several types of wireless networks, each serving specific purposes and ca-tering to different connectivity needs. Here are some commonly used types of wire-less networks:

Wi-Fi (Wireless Fidelity) networks are widely used for local area networking (LAN) in homes, offices, public spaces, and other environments. They provide wireless internet access to devices within a specific coverage area. Wi-Fi networks operate on various IEEE 802.11 standards, such as 802.11ac (Wi-Fi 5) and 802.11ax (Wi-Fi 6) [4]. Cellular Networks enable wireless communication over long distances using cellular towers. These networks are used for mobile telephony and data services. They include generations such as 2G, 3G, 4G LTE, and the latest 5G, offering increased speeds, lower latency, and enhanced capacity.

Bluetooth technology is designed for short-range wireless communication between devices. It is commonly used for connecting peripherals like keyboards, mice, headphones, and speakers to computers, smartphones, and other devices in close proximity. Bluetooth is also utilized in IoT devices for data transfer and control. Zigbee is a wireless technology used for low-power, short-range communication between devices. It is commonly employed in home automation, smart lighting systems, and industrial applications where devices need to communicate wirelessly over a limited range.

AI-based reliable and secure data transfer refers to the use of artificial intelligence (AI) techniques and technologies to enhance the reliability and security of transferring data between systems or devices. It involves leveraging AI algorithms and approaches to optimize data transfer processes, improve data integrity, protect against unauthorized access, and ensure the confidentiality of sensitive information.

1.1 AI Contribution Towards Reliable and Secure Data Transfer

Error Correction and Data Integrity

AI algorithms can be used to implement error correction codes and techniques that help identify and correct errors that may occur during data transmission. These algorithms

can detect and reconstruct corrupted or lost data, ensuring the integrity of the transferred information.

Predictive Analytics and Quality of Service (QoS)
AI can analyze historical data on network performance and behavior to predict potential network disruptions or congestion. By considering factors like bandwidth availability, latency, and network load, AI systems can optimize data transfer by dynamically selecting the most suitable routes and protocols for efficient and reliable data transmission.

Intrusion Detection and Prevention
AI-powered systems can employ machine learning techniques to analyze network traffic patterns and detect anomalies or potential security threats. By continuously monitoring network activities, AI algorithms can identify and respond to suspicious behavior, helping to prevent unauthorized access, data breaches, or malicious attacks during data transfer.

Data Encryption and Privacy
AI can be utilized to develop robust encryption algorithms and privacy-enhancing techniques. Encryption mechanisms, such as symmetric and asymmetric encryption, can be applied to data at rest or in transit, ensuring that sensitive information remains secure and protected from unauthorized access.

Behavioral Analysis and User Authentication
AI systems can employ behavioral analysis techniques to recognize patterns in user behavior during data transfer. This can help detect unauthorized access attempts or unusual activities, triggering additional security measures or authentication processes to ensure the authenticity of users and devices involved in data transfer.

Threat Intelligence and Real-Time Monitoring
AI can leverage threat intelligence feeds and real-time monitoring to identify and respond to emerging threats or vulnerabilities. By integrating AI-based security solutions, organizations can proactively mitigate risks and ensure the secure transfer of data by staying ahead of potential threats [5]. By integrating AI into data transfer processes, organizations can enhance reliability, reduce data loss, minimize the risk of security breaches, and optimize the overall performance of their networks. However, it's important to note that implementing AI-based security measures should be done in combination with other established security practices and standards to create a robust and comprehensive data transfer environment.

Wireless networks face several challenges that can impact their performance, reliability, and security [6]. Some of the common challenges in wireless networks operate in shared frequency bands, making them susceptible to interference from other devices and networks operating in the same frequency range. Interference can degrade signal quality, reduce throughput, and cause connectivity issues. Signal Attenuation and Range Limitations in wireless signals are subject to attenuation, meaning their strength diminishes as they propagate through space. Obstacles like walls, buildings, and distance can further

limit the range of wireless networks and weaken signal strength, resulting in reduced coverage and performance.

Bandwidth Constraints in wireless networks typically have limited bandwidth compared to wired networks [7]. As the number of connected devices and data-intensive applications increases, it can lead to congestion and reduced network performance.

Security Risks in wireless networks are vulnerable to security threats, such as unauthorized access, eavesdropping, data interception, and network intrusion. Weak encryption, poor authentication mechanisms, and unsecured configurations can expose networks to attacks and compromise the confidentiality and integrity of transmitted data.

Mobility and Handover in wireless networks introduces challenges related to seamless handover as devices move between different access points or cells. Maintaining a stable connection during handover is crucial to avoid disruptions in ongoing communications.

Quality of Service (QoS) Management ensuring consistent QoS is challenging in wireless networks, especially in environments with varying signal strengths or high user densities. Factors like latency, packet loss, and jitter can affect the performance of real-time applications like voice and video streaming.

Power Consumption in wireless devices, particularly battery-powered devices, need to manage power consumption efficiently to prolong battery life. Balancing power-saving techniques with the need for reliable connectivity and performance is a challenge in wireless networks.

Scalability is the number of connected devices increases, scaling wireless networks to accommodate the growing demand becomes a challenge. Network architectures and protocols need to support large-scale deployments without sacrificing performance or reliability.

Standards and Compatibility in wireless networks rely on various standards and protocols, and compatibility issues can arise when devices from different vendors or generations attempt to connect or communicate. Ensuring interoperability and seamless integration across devices and networks can be a challenge. Regulatory Compliance in wireless networks must comply with regulatory requirements governing spectrum allocation, power limits, and security protocols [8]. Adhering to these regulations while maintaining optimal network performance poses challenges for network administrators.

Efforts are continuously made to address these challenges through advancements in wireless technologies, improved network design, enhanced security measures, and ongoing research in areas like spectrum management, signal processing, and network optimization.

Wireless data transfer introduces unique security challenges due to the open nature of wireless communication. However, several techniques are employed to ensure data security in wireless transfer. Here are some commonly used techniques:

Encryption is a fundamental technique used to protect data during wireless transfer. It involves encoding the data in such a way that it can only be decrypted and understood by authorized recipients. Common encryption algorithms used in wireless networks include AES (Advanced Encryption Standard) and WPA2 (Wi-Fi Protected Access 2).Authentication techniques verify the identities of devices and users involved in wireless data

transfer. This ensures that only authorized parties can access and transmit data. Techniques such as passwords, digital certificates, and biometric authentication are used to authenticate devices and users in wireless networks.

2 Literature Survey

By examining the methodologies, approaches, and research designs employed in previous articles referred several papers as follows. One paper titled Reliable and secure data transfer in IoT networks delas about IoT ecosystem novel distributed key management technique [9]. The suggested approach efficiently protects IoT devices by offloading the majority of resource-intensive cryptographic operations to a local entity. The following sub networks are used in this suggested strategy to take advantage of mobile agents to process the IoT devices' cryptography work and undertake a quick authentication procedure by posing as a local authorized entity. Application security and user security are two subcategories of information transmission security concerns. User security is primarily concerned with safeguarding the security of the user's sensitive data, as opposed to application security, which focuses on data protection when a user uses a particular programmer. Our concept provides security based on an MA's prediction of mobility in a sub network of an IoT network [10]. When the main IoT application is started at the beginning of a session at a sub network, the SA issues a certificate to the user device. There are a few issues with the proposed model that we plan to solve in more exploration. For anomaly detection, rigid rules set by humans are utilized initially. As a result, locating unknown abnormalities outside of the gathered variables is a challenging task. Second, an end-to-end evaluation of the proposed strategy requires real-world testing. Further testing and a reconfiguration of the suggested strategy are required. Third, depending on the complexity of the algorithms, human judgement is utilized to choose which algorithms to apply on various devices.

Other paper titled Distributed AI-Driven Search Engine on Visual Internet-of-Things for Event Discovery in the Cloud.In this paper, they propose distributed deep neural networks (DNNs) over edge visual Internet of Things (VIoT) devices for real-time video scene parsing and indexing in conjunction with Big Query retrieval on cloud-stored data. A method for generating useful representation from raw data that a camera outputs in the form of video is called video analytics [11]. An intelligent video analytics system will be able to narrow the search by employing a range of criteria and create a knowledge base that is more reliable and accurate for making judgments and, eventually, taking action. The proposed architecture bridges the edge-to-cloud gap by judiciously allocating the AI workload between the edge and the cloud. Video security cameras and other stream-ing media may be seamlessly incorporated into smart cities thanks to the Visual Internet of Things (VIoT). However, working with and gaining insight from such a large amount of data is challenging.

One of the major contributions taken from the paper titled Securing Big Data: A Survey on Security Solutions deals about there are many security risks that could affect the confidentiality and integrity of data that is sent, processed, and stored. Numerous methods have been created to address these security challenges and worries [12]. This survey article's goal is to identify and describe the security concerns connected to the

Big Data architecture. Due to its promising features, cloud computing (CC) has been chosen as the infrastructure for BDA. However, the conceptual taxonomy of security and privacy for the BD framework's four primary objectives are data confidentiality, data provenance, system health, and public policy, social, and cross-organizational concerns [13]. The importance of BDA has grown, which has prompted the development of many BD security frameworks for handling massive amounts of data. Hosting BD frameworks necessitates a trustworthy and secure infrastructure provider, CIA, to meet the essential security standards. This article gave a general review of BDA-related research from the security point of view, covering the BD lifecycle, security challenges, and worries. The study described the widely used security measures to protect the BD framework. It was clear that encryption and its alternatives surpassed the bulk of the proposed solutions and showed their effectiveness.

3 Proposed Methodology

In order to improve the security in the wireless networks the best way is to use Authentication technologies. To satisfy different use cases and demands, varied authentication techniques are needed to provide security and ease to your users. To satisfy the various demands, we provide a variety of user authentication techniques.

The process of asking for specific credentials, such as a username and password, in order to determine whether or not a user trying to access network resources is authorized. In addition to other areas, authentication can be enabled on console ports, AUX ports.

As network administrators, we have the authority to control how a user is authenticated when they attempt to access the network [14]. These methods include using the router's internal database and sending authentication requests to a distant server, like the ACS server. To choose the authentication method to be used, a default or customized authentication method list is used.

By considering these comparisons we have to select that user id and password-based Au-thentication and OTP based Authentication to improve the security and develop as multi factor Authentication. Because in the multi-factor authentication we have to use more then one authentication method. If we consider the all the possibilities that we have the best one combination of OTP based and user-ID based. Because in the user-id based only the security is poor but remaining are better to use. So to improve the security we can go with OTP based even though token based has higher security then OTP token based is difficult to deploy then the OTP based so it is better to go with the OTP based then the token based.

In the proposed methodology the multi factor Authentication is done by deploying the two layers of authentication in the 1st layer we use the user id and password-based Authentication. Because the user will have their own user credentials to enter the network. And it is easy to use and deploy [15]. So that the 1st layer of authentication is done by using the user-id based authentication. And coming to the 2nd layer of authentication we can use OTP based authentication. In this layer the user will initially register with mail-id or phone number, an OTP is sent to the registered phone number or mail-id. By entering the OTP received by the user the network will consider the user as the legal user and give the access to the network. If the user has entered the incorrect OTP, then

the user will another OTP. This process will repeat until the user has to enter the correct OTP.

The next challenge that we consider is its dynamic architecture and functional analysis of the network. For this we used the shortest-path tree algorithm to find the best path in the network. By finding the best path we can it is easy to send the data from source to destination. You may determine the shortest path between two nodes in a network using Dijkstra's Algo-rithm. It create a shortest-path tree by determining the shortest path from a node (referred to as the "source node") to every other node in the graph.

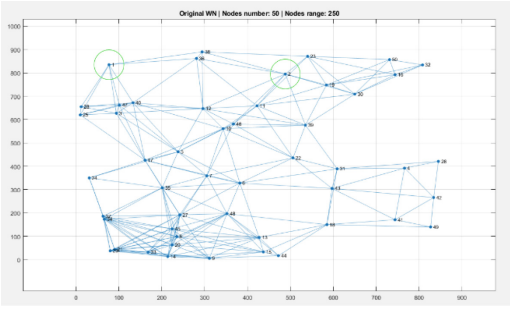
To determine the quickest route between the present location and the destination, GPS devices employ this method. It has several industrial uses, particularly in fields where modelling networks is necessary. To use this algorithm, we have to give wights. Here we are taking the distance between each node as the weights For that case the distance will be find using the Euclidean distance formula shown in Eq. 1.

$$\sqrt{(a2 - a1)^2 + (b2 - b1)^2} \tag{1}$$

By using the formula, the distance is measured between distance each node present in the network and the distance values in the form of tables. These distance tables are used in the analysis of the network architecture and find the neighbor nodes to each node present in the network as per the node range given by the user.

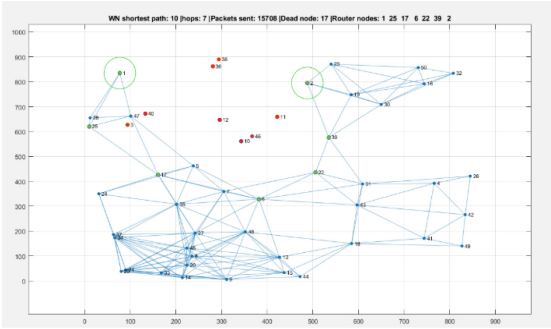
4 Results and Discussion

The biggest challenge that we consider in the wireless network is dynamic architecture analysis. For that we have developed a MATLAB algorithm. To find the neighbor nodes to each node and find the shortest path between the source and destination.

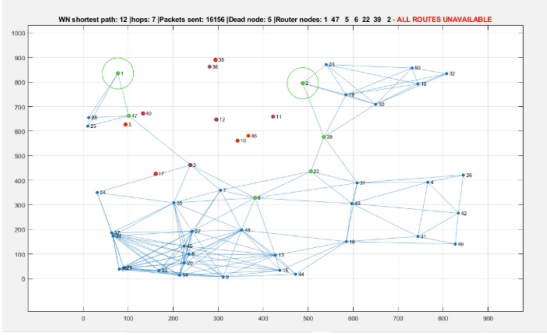


Original network

The above network is the given dynamic network in which have to do the analysis. Where the node 1 is the source node in the network and the node 2 is the destination node in the network.



Leaving dead node and find alternate path (after 9 stages)



All routes are unavailable

By observing the behavior of the nodes present in the network we can get the deep analysis of the network in this simulation we only consider the distance. But in the case of we have to consider the remaining terms like cost, number of nodes present between the source and destination, bandwidth. Then we will get the complete analysis of the network.

5 Conclusion and Future Scope

This paper mainly focus on how AI can play a crucial role in enhancing the reliability and security of data transfer in wireless networks and identifying the best authentication method for data transfer involves considering various factors related to security, usability, and the specific requirements of the data transfer scenario. In this work proposed few steps where these challenges are arising in the wireless networks. The main challenge in the wireless network is the illegal users are entering to the network and accessing the data (security). And due to its dynamic nature, the nodes present in the network are not stationary. Ultimately, there is no one-size-fits-all approach to authentication for data transfer. The best method will depend on the specific needs of your organization, the type of data being transferred, and the level of security required. It may also involve combining multiple authentication methods (multi-factor authentication) for enhanced security.

References

1. Dannana, S., Prabakaran, T., Rajasekaran, A.S., Kumareshan, N., Shadrach, S.F.D., Kalyanchakravarthi, P.: A novel system model for managing cyber threat intelligence. In: 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon) (2022). https://doi.org/10.1109/mysurucon55714.2022.9972703
2. Das, A., Roopaei, M., Jamshidi, M., Najafirad, P.: Distributed AI-Driven search engine on Visual Internet-of-Things for event discovery in the cloud (2022).https://doi.org/10.1109/sose55472.2022.9812698
3. Habbak, H., Metwally, K., Mattar, A.M.: Securing big data: a survey on security solutions. In: Inter-national Conference on Electrical Engineering (2022).https://doi.org/10.1109/iceeng49683.2022.9781955
4. Martins, O., et.al.: Artificial intelligence techniques for cognitive sensing in future IoT: state-of-the-art, potentials, and challenges. IJ. Sens. Actuator Netw. **9**, 21 (2020). https://doi.org/10.3390/jsan9020021
5. Akpakwu, G.A., Silva, B.J., Hancke, G.P., Abu-Mahfouz, A.M.: A survey on 5g networks for the Internet of Things: communication technologies and challenges. IEEE Access **6**, 3619–3647 (2018)
6. Chakraborty, C., Rodrigues, J.J.: A comprehensive review on device-to-device communication paradigm: trends, challenges and applications. Wirel. Personal Commun. **114**, 185–207 (2020).https://doi.org/10.1007/s11277-020-07358-3
7. Doppler, K., Rinne, M., Wijting, C., Ribeiro, C., Hugl, K.: Device-to-device communication as an underlay to LTE-advanced networks. IEEE Commun. Mag. **47**, 42–49 (2009)
8. Ali, K.S., ElSawy, H., Alouini, M.S.: Modeling cellular networks withfull-duplex D2D communication: a stochastic geometry approach. IEEE Trans. Commun. **64**, 4409–4424 (2016)
9. Migabo, E., Djouani, K., Kurien, A.: An energy-efficient and adaptive channel coding approach for narrowband Internet of Things (NB-IoT) systems. Sensors **20**, 3465 (2020). https://doi.org/10.3390/s20123465
10. Miao, Y., Li, W., Tian, D., Hossain, M., Alhamid, M.: Narrow band Internet of Things: simulation and modelling. IEEE Internet Things J. **5**, 2304–2314 (2018)
11. Li, S., Xu, L.D., Zhao, S.: The Internet of Things: a survey. Inf. Syst. Front. **17**, 243–259 (2015)
12. Yu, C., Yu, L., Wu, Y., He, Y., Lu, Q.: Uplink scheduling and link adaptation for narrowband in-ternet of things systems. IEEE Access **5**, 1724–1734 (2017)
13. Palattella, M.R., et al.: Internet of Things in the 5G era: enablers, architecture, and business models. IEEE J. Sel. Areas Commun. **34**(3), 510–527 (2016)
14. Gochhayat, S.P., et al.: Reliable and secure data transfer in IoT networks. Wirel.Netw. **26**(8), 5689–5702 (2019). https://doi.org/10.1007/s11276-019-02036-0
15. Da Xu, L., He, W., Li, S.: Internet of Things in industries: a survey. IEEE Trans. Ind. Informat. **10**(4), 2233–2243 (2014)