ARTIFICIAL INTELLIGENCE OF THINGS (AIOT)

Abstract

With this new trend in computer science, new technologies are being developed with new evolutions. The Internet of Things is the best way to communicate with devices with unique capabilities. The Internet of Things (IoT) is a new technology that connects various devices and objects. Here, Chapter 1 covers IoT using artificial intelligence, importance of IoT using artificial intelligence, advantages of AIoT systems, how AI transforms IoT, IoT and sensor networks, safe and secure I have to mention that it introduces IoT using artificial intelligence in the environment. efficient authentication.

Keywords: AIoT, sensor networks, aviation networks, traffic management, machine learning.

Author

Ms. Priyanka Nanda
School of Computational Science
GNA University, Punjab, India

I. INTRODUCTION

Artificial Intelligence of Things (AIoT) combines Artificial Intelligence (AI) technology with Internet of Things (IoT) infrastructure. The goal of AIoT is to improve data management and data analysis, restore human-machine interaction, and organize IoT operations.AI, which is frequently utilized in speech recognition, machine vision, and natural language processing, is the reproduction of human intelligence processes by computers, particularly computer systems. IoT refers to mechanical and digital linked computing equipment with unique identities that may send data via networks without the requirement for a human-to-human or human-to-computer interaction. is a division of equipment or things. The Internet of Things (IoT) encompasses any device that can be given an internet protocol address and transmit data over the network, such as a human implanted heart monitor or a car with built-in sensors that warn the driver when tire pressure is low.TheAIoT is a reformulation and both types of technology have common uses. AI adds value to the Internet of Things through machine learning capabilities and improved decision-making processes, while IoT adds value to AI through connections, waves, and data sharing. AIoT can improve your business and its services by creating more value from IoT-generated data. AI will enable IoT devices to use collected big data to improve analysis, learning, and decision-making without the need for humans.

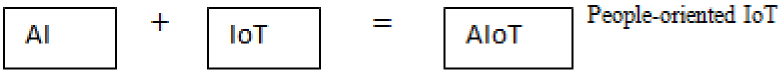

Figure 1: Artificial Intelligence of Things

1. **Importance of AIoT:** IoT is an emerging field and most trending technology now-a-days. AI-integrated IoT devices can analyze data to divulge patterns and insights and adjust system operations to be more competent. In AIoT, data can be generated and analyzed to identify points of failure, allowing the system to make adjustments as needed. In AIoT, employees do not have to spend as much time monitoring IoT devices, saving money and time. The numbers of devices connected to an IoT system can be improved to optimize existing processes or introduce new functions. Today, IoT-connected sensors are already being used to control lighting, utilities, air conditioning, access, and more. Grouping by AI algorithms can recognize energy management and efficiency plans to create a more sustainable environment as well as a more comfortable and safer environment for humans. Below are various applications using AIoT:

   - **Smart Cities:** Smart cities enable centralized management of urban areas and services such as traffic, transport, charging stations, waste management, lighting, parking, and environmental quality. Sensors placed in each area or service transmit data via the IoT, which is collected and processed by artificial intelligence to identify patterns and trends that, after analysis, enable forecasting and/or forecasting of future flows and demand. cities to function more efficiently and reduce their environmental impact.

   - **Smart Industry:** In smart industry, the possibilities are even wider. The benefits of deploying AIoT systems include increased efficiency, increased productivity, resource savings, and even reduced carbon emissions. In addition, the technology is industry-agnostic and can be used by all types of companies, from SMEs to multinational industrial corporations. Real-time, interconnected IoT systems generate massive amounts of data that can be processed and analyzed by AI algorithms, turning them into valuable information, enabling managers and middle managers to make better decisions based on more accurate data. can make good decisions.

- **Intelligent Traffic:** Road congestion may be annoying in a variety of ways. Longer wait times, fuel waste, and increased pollutants result from this. Any logistics organization must consider routes before making any decisions. Truck drivers could get stuck in lengthy traffic jams on congested roadways if they lack trustworthy information. His usage of AIoT in intelligent transportation therefore becomes increasingly crucial to boost productivity. In the field of smart transportation, embedded devices in the IoT ecosystem are capable of analyzing weather patterns, traffic patterns, and other variables to address practical issues. Companies may now use embedded software to permanently reduce traffic congestion.

II. ENEFITS OF AIOT SYSTEMS IN TRAFFIC MANAGEMENT

AIoT improves traffic safety by incorporating a variety of previously unavailable data. Various advantages of this system are listed below:

1. Collection and real-time relaying of traffic numbers.
2. Reduction of waiting time at traffic lights and highways.
3. Proactive traffic management despite dynamic conditions.
4. Finding an appropriate balance between traffic densities.
5. Reduced carbon monoxide emissions.f. The system minimizes the margin for error, thus improving road safety.

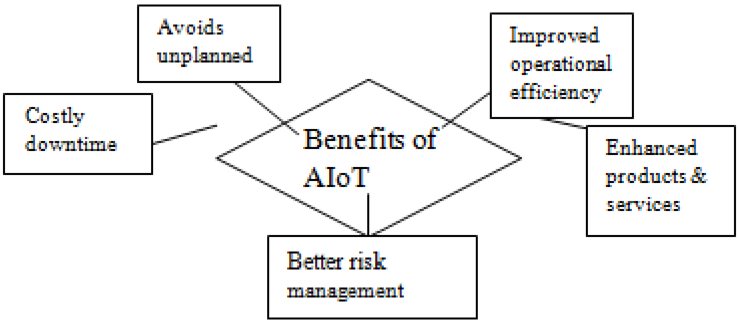

Figure 2: Benefits of AIoT

III. IMPACT OF AI ON IOT

Over the last few decades, the business world has witnessed a steady adoption of the Internet of Things (IoT). With advances in artificial intelligence (AI) and machine learning (ML) curtailing the ability of his IoT devices to leverage "artificial intelligence of things" (AIoT), the next wave of IoT evolution is leading us . AI is transforming the Internet of Things by making it easier for people to interact with their devices. The Internet of Things is changing the face of technology through data collection and analysis from connected devices. Artificial Intelligence (AI) and Machine Learning (ML) are his two major technologies that enhance IoT in terms of responsiveness and automation of user experience systems.Artificial Intelligence (AI) allows machines to learn how to perform tasks based on new data inputs. Machine learning (ML) enables computers to analyze data more quickly and recognize patterns for future predictions. Machine learning (ML) and artificial intelligence (AI) are both having a significant influence on a number of industries, including healthcare, retail, logistics, finance, and agriculture. A technological advancement that can enhance the functionality of your smartphone is artificial intelligence. To benefit from AI, IoT devices do not need to be as sophisticated as PCs. IoT networking has the potential to increase AI adoption in a number of ways. One approach is to make IoT devices capable of comprehending spoken language.

Example: When you turn on your air conditioner with the remote control, it understands your language. That's because the device uses AI to understand human speech. So you don't have to press another button to adjust the air conditioner. You can easily adjust the room temperature with voice commands. IoT devices are interconnected and connected to the internet so all his IoT data can be collected. There are various data about sensors that can be used more effectively with the help of artificial intelligence. As such, it can be used in IoT devices to make them smarter and more efficient. It can also greatly improve the productivity and efficiency of IoT devices. It can be used both to respond to human commands and to perform tasks autonomously.

IV. IOT V_S SENSOR NETWORKS

A wireless sensor network (WSN) is a group of autonomous devices that forms an ad hoc network to collect data from the real world. It is made up of a number of sensor networks. Body Area Networks (BAN), Field Area Networks (FAN), Mesh Networks, and Narrowband IoT (NB-IoT). These gadgets employ certain communication protocols and have minimal power consumption. Each of these individually linked devices must provide data for collection and analysis by IoT systems. While private cloud providers only serve a small number of clients, public cloud providers supply apps and storage. A sensor network installed on a boat's hull to detect floods is one example of a WSN. Each sensor in this situation has a distinct ID and operates independently.

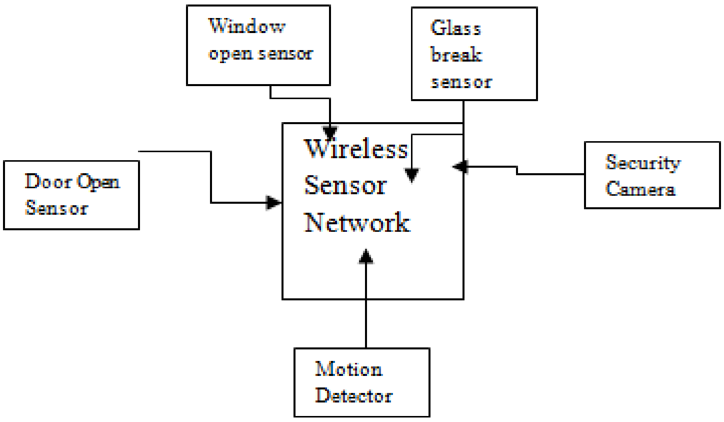

Figure 4: Wireless Sensor Network

The Internet of Things (IoT) is a network of physical objects equipped with sensors, software, and other technologies to connect and exchange data with other devices and systems over the Internet. The term IoT greatly improves the approach by which we can control and monitor all the processes running in our homes. IoT-based home security systems allow users to monitor and manage home security, such as door access and monitoring. Smart home systems provide efficient energy through the use of smart lighting. Smart home systems require the use of intelligent algorithms that give appliances a degree of autonomy. It has energy calculation parameters that allow communication and collaboration with smart objects. For improvement, hybrid intruder detection systems and edge computing should be proposed. We offer automatic, safe, energy-efficient, cost-effective and reliable smart home solutions based on edge computing capabilities. IoT-based home automation requires the use of sensors to control sound and lighting systems and automatically turn fans on and off. Home automation is the ability to operate home appliances using internet-connected tools. In addition to home automation, we must use home security systems to ensure the protection of our homes. IoT-based home security systems allow users to monitor and manage home security, such as door access and monitoring. Owners can also capture images of intruders trying to access the door. The door opens as soon as a suitable person is detected using sensors. The smart home system also ensures energy efficiency through the use of smart lighting, but also requires the use of smart his algorithms that give home appliances a degree of autonomy. It has various parameters for calculating energy, and can communicate between networks and work with smart objects. For improvement, we proposed hybrid IDS and edge computing. A hybrid IDS consists of anomaly and fraud detection modules. Detecting and responding to cyber-physical attacks with a DER system is more effective.

Table 1: IoT vs. Wireless Sensor Network

Basis	IoT	Wireless Sensor Network
Architecture	A gateway for IOT is able to connect to internetworks (which contain routers, switches, APs, etc.	WSN is a network made up entirely of sensors.
Devices	IOT uses IPv4 for the internetwork part and IPv6 for the sensor network (802.15.4 MAC/PHY).	WSN utilizes IPv4 and has a sink rather than a gateway.
Protocols	AODV and RPL are two routing technologies included in NetSimIoT	The NetSim WSN uses the following routing protocols: DSR, AODV, OLSR, and ZRP.

V. AERIAL AND SPACE NETWORKS

Space networks are the program that is under NASA which combines space and ground elements to support spacecraft communications. It can include the following things:

- The geosynchronous Tracking and Data Relay Satellites(TDRS)
- Supporting ground terminal systems
- The Bilateration Ranging and Transponder System
- Merritt Island Launch Annex(MILA) relay
- Network Control Center Data System (NCCDS)

The space information networks are incorporated networks based on various space platforms including GEO, M/LEO satellites, and airships on high altitude platform stations (HAPSs) to support real-time communications, massive data transmission and processing, and systematize information services. Compared to terrestrial networks, space information networks have broader application areas and wider coverage, which may expand human activities to space, high seas, and even outer space. Due to the unique features (i.e., high altitude, wide coverage, and line-of-sight transmission) of space information networks, they are expected to play a key role in the applications of communications, remote sensing, air traffic control, aviation/maritime communications, Internet of Things (IoT), and aerospace measurement. Particularly, space information networks become more significant and indispensable to construct Internet infrastructures in remote areas of the globe and provide emergency communication services in case of natural disasters (hurricanes, earthquakes, floods, etc.). However, due to limited spectral, energy, and orbital resources, expanding the spatiotemporal range poses many theoretical and technical challenges to the development of space information networks.

1. Difference between Conventional and Wireless Communication Systems:

- **Wired / Wireless:** Conventional and wireless are two different communication systems. A very noticeable difference is the presence of wires in traditional communication systems. The technologies used in both system infrastructures, such as the core elements of network services, are the same. Wired networks communicate over wires, while wireless communication systems use radio waves

- **Complicated / Non-complicated**: While traditional wired communication systems are easy to install and repair, wireless communication systems are complex to set up. Its maintenance and troubleshooting are impossible without experts.

- **Mobility/Immobility:** Immobility is a major drawback of wired communication systems, making it difficult to leave your seat in any situation. Wireless communication systems facilitate mobility, allowing you to sit and work wherever you like.

- **Expensive/Cheap:** Wired has additional costs for wiring and cables, which puts pressure on the budget, but wireless has no wiring troubles and is very affordable.Speed: Wired network transmission speed is better than wireless system. Wired systems don't require shared storage, so there's no need for a user interface. Wireless communication systems sometimes need to share a band with multiple users, which can slow transmission speeds.

- **Seen / Unseen:** Wireless systems are of insecure interest, such as invisible data transmission using radio waves (commands such as playing and sharing music, printing documents, sharing files, etc.). Other examples of wireless communication systems include Bluetooth and cordless phones.

- **Reliability:** Traditional communication systems such as cable and Ethernet are available in their most powerful form, as they promise good speeds of nearly 1000Mbps, faster than all other connection types. As an improvement in security.

And getting high speed and security at an affordable price is not a big deal. Wired systems are therefore more reliable than wireless systems.

- **Home/Business:** The wireless network works well and speed is not a big issue, so it can be a good choice for home users. However, in office environments, wired communication systems are preferred due to the need for high speed data transmission and security. But as offices become more mobile, they need wireless systems to transmit portable data. Wireless systems don't have the hassles of wired systems. The wireless system is easy to install as it connects instantly via wireless USB. To change the location of the system in your office, simply use the map to move the system to the desired location.

- **Hotspot:** Hotspot is becoming a common term for wireless systems. The Owner provides the Internet to users as a promotional package in public places, libraries, hotels, schools, airports, train stations, etc. in order to promote their use and attract users. If it's a wired network, you can only access the internet via cable and there is no concept of hotspots.

- **Quality of Service (QoS):** The downside of wireless communication is Quality of Service (QoS). There is no guarantee that you will always receive a strong signal, as changes in the environment and other obstacles (walls, birds, aircraft) can interrupt the signal. Virtual Network An advantage of wireless communication is the form of WLAN that creates a virtual network for users near universities and libraries. Provides wireless internet access. No access point required.

2. **Non-Conventional Methods of Communication:** Following are the different ways to communicate:

- **Visual Arts:** Words, whether written or spoken, are not always the best way to communicate. Art can be a great alternative. Painting, painting, and sculpting are better ways of communicating. After all, pictures say more than a thousand words. Presenting a work of art is a quicker and more effective way to get your message across than using text boxes. This is why billboards and magazine ads have been used as a marketing tool for many years, and why logos are so much a part of our daily lives. Whether it's the classic golden arches of McDonald's or the swooping white swoops of Nike, consumers of all ages instantly evoke positive memories and reactions.

- **Music Sound:** Can communicate much like visual art. Music is an accessible form of communication available to everyone. Written music can be read across cultures and continents. Music can express anger, happiness, peace and sadness. Music can even beat dementia, according to the Mayo Clinic. Music therapy can improve the quality of life of people with dementia because it provokes deep feelings of joy.

- **Letters:** The old "snail mail" letter was one of the most important means of communication. In the age of the Internet, handwritten letters are no longer so popular. This creates a unique opportunity for unforgettable communication. Writing letters and notes by hand is a conscious and personal effort. There is also room for creativity in letters. Write on customized stationery, draw pictures, and write in multiple colors of ink. The tactile sensation of opening the letter and seeing bright and beautiful colors emerge from the paper makes the reader feel happy. Handwritten letters can actually improve customer relationships, according to Entrepreneur.com.

- **Haptic Communication:** It doesn't take a degree in communications to understand how tactile experiences are linked to memory. Yet the use of touch is an often overlooked form of communication. This type of communication takes many forms. Pat them on the back instead of shouting for attention, pick up what they want instead of pointing at it, or hold someone's hand. Haptic communication is a simple but effective way to make new ideas and shopping lists more memorable.

- **Sports and Games:** Sports are so popular in American culture that the unique Bachelor of Sports Communication degree is awarded. Sports are used to improve social skills with youth teams, to create a better environment in the office, or simply to bring people together in front of the TV. Gaming is also a growing hobby, with more people playing video and board games than ever before.

VI. ARTIFICIAL INTELLIGENCE IOT IN SECURE AND EFFICIENT AUTHENTICATION

With fast-evolving cyber assaults and the speedy multiplication of gadgets taking location currently, AI and desktop studying can assist to hold abreast of cybercriminals, automate risk detection, and reply greater efficiently than traditional software-driven or guide techniques. Security and authentication will proceed to enhance and end up smarter. Eventually, authentication will possibly go from supervised learning, the place the dataset consists of the outcomes, to unsupervised gaining knowledge of the place AI finds new patterns that human beings may additionally no longer have determined and makes predictions of plausible elements to assess. Being capable to pass reference more than one desktop studying algorithms and use sample cognizance and time-series primarily based predictive algorithms will enhance the accuracy and scope of AI-based authentication choices going forward, for net software logins, however additionally for different factors of cybersecurity such as community intrusion and botnet detection. AI develops extra positive algorithms to decide which elements point out an assault via making an attempt one of a kind strategies to resolve issues and checking its reply towards the reply in the dataset. Finally, we discover a set of algorithms that can precisely predict threats in most cases.

Following are the some points based on security and authentication regarding Artificial Intelligence IoT:

- Secure and Efficient Privacy Preserving Set Interfaces with Identity Authentication in IoT.
- Artificial Intelligence in Efficient Privacy Preserving Anonymous Authentication Schemes for Human predictive Online Education Systems.
- Quantum Secure Authentication and Key Agreement Multi-Agent AI Public Cloud in Interaction.
- Secure facts trade algorithms that guard the privateness of the public IoT cloud.

- AI for environment friendly authenticated team key settlement protocol for dynamic UAV fleets in untrusted environments.

1. **Authentication and Authorization:** Authentication is the method of machine identification, whilst authorization gives permissions. IoT gadgets use these tactics to do role-based get admission to manipulate and make sure that units solely have get admission to and permission to do precisely what they need. Only licensed units can have interaction with different devices, applications, cloud money owed and gateways.

   Administrators register every system when they installation it on the system. The gadget validates gadgets when they join and share data. Many businesses use public key infrastructure (PKI) to hyperlink gadgets with public key certificates from certificates authorities to assign and affirm gadget identities. PKI establishes an IoT device's legitimacy on a community to share data.

2. **Authentication and Authorization models and Types:** There are two types of models:

   - **Distributed Model:** The distributed model defines a way of contact in between the aspects of a device and it refers to how sources are unfold out and works on extra than one system to enhance the effectiveness and overall performance of a task. The disbursed fashions are used in many areas; some are:

     - **Distributed Database Mannequin:** It specifies that the storage is now not connected in a single frequent processor; it may also shop in many computer systems which may additionally be positioned in special locations.
     - **Distributed Community Mannequin:** It specifies that the networking device is unfold out for the pc application and the facts throughout extra than one pc that make use of low value laptop electricity and function the information extra efficaciously with a combine of desktops.
     - **Distributed Computing Mannequin:** It specifies to share the aspect of a software program device in a dispensed manner to enhance the effectivity and recital.
       - Problems on designing a allotted model.
       - Usage of broadly various modes.
       - Wide vary of device environments.
       - Internal hassle and exterior threads.

   Distributed Model is additionally recognised as mutual authentication, this protocol is used when each units authenticate every different earlier than they communicate. Each system should have a great digital identification saved for the different machine and then evaluate identities. The gadgets can solely join when the first system beliefs the 2d device's digital certificates and vice versa. The Transport Layer Security protocol exchanges and compares certifications.

   - **Centralized Model:** Centralized Model tells the strategic planning, purpose setting, budgeting, and Genius deployment are generally carried out by means of a single, senior chief or management team. In contrast, in decentralized organizations, formal decision-making electricity is allotted throughout a couple of humans or teams. In centralized model, it is used to focal point with the aid of setting electricity and authority in a middle or central organization. centralized a number of features in a single agency.

In the authentication mannequin of centralized, an admin registers the units with a central authority or server and connects the gadgets with legitimate digital certificates. The central authority simplifies the impervious handshake between the two gadgets that desire to communicate. In three-way authentication, the safety certificates don't seem to be saved on the units and can not be stolen by using criminals, but the gadgets nevertheless have sturdy security. This methodology works first-rate for always-connected gadgets or ones with on-demand net get entry to due to the fact it eliminates any authentication delay. A certificates and key lifecycle administration provider can control the certificates centrally and join to any system on a community that desires verification.

REFERENCES

[1] R. S. Michalski, J. G. Carbonell, and T. M. Mitchell, Machine Learning: An Artificial Intelligence Approach. Springer Science & Business Media, 2013.
[2] I. H. Witten and E. Frank, Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann, 2016.
[3] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, and K. Ueda, "Cyber-Physical Systems in Manufacturing," CIRP Annals, vol. 65, no. 2, pp. 621–641, 2016.
[4] E. A. Lee and S. A. Seshia, Introduction to Embedded Systems: A Cyber-Physical Systems Approach. MIT Press, 2016.
[5] Q. F. Hassan, A. R. Khan, and S. A. Madani, Internet of Things: Challenges, Advances, and Applications. Chapman & Hall/CRC Computer and Information Science Series, CRC Press, 2017.
[6] G. Fortino and P. Trunfio, Internet of Things based on Smart Objects: Technology, Middleware and Applications. Springer, 2014.
[7] L. T. Yang, B. Di Martino, and Q. Zhang, "Internet of Everything," Mobile Information Systems, vol. 2017, 2017.
[8] R. Baheti and H. Gill, "Cyber-Physical Systems," The Impact of Control Technology, vol. 12, pp. 161–166, 2011.
[9] M. M. Gorman, Database Management Systems: Understanding and Applying Database Technology. Elsevier Science, 2014.
[10] S. Theodoridis and K. Koutroumbas, Pattern Recognition. Elsevier Science, 2008.
[11] N. Marz and J. Warren, Big Data: Principles and Best Practices of Scalable RealTime Data Systems. Manning, 2015.
[12] J. Leskovec, A. Rajaraman, and J. D. Ullman, Mining of Massive Datasets.Cambridge university press, 2014.
[13] J. Fan, F. Han, and H. Liu, "Challenges of Big Data Analysis," National Science Review, vol. 1, no. 2, pp. 293–314, 2014.
[14] P. Zikopoulos, C. Eaton, et al., Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data. McGraw-Hill Osborne Media, 2011.
[15] A. Ghosh, N. S. Mishra, and S. Ghosh, "Fuzzy Clustering Algorithms for Unsupervised Change Detection in Remote Sensing Images," Information Sciences, vol. 181, no. 4, pp. 699–715, 2011.
[16] A. Halder, S. Ghosh, and A. Ghosh, "Aggregation Pheromone Metaphor for SemiSupervised Classification," Pattern Recognition, vol. 46, no. 8, pp. 2239–2248, 2013.
[17] D. Cohn, "Active Learning," Encyclopedia of Machine Learning and Data Mining, pp. 9–14, 2017.
[18] S. Jha and S. A. Seshia, "A Theory of Formal Synthesis via Inductive Learning," ActaInformatica, vol. 54, no. 7, pp. 693–726, 2017.
[19] S. J. Pan and Q. Yang, "A Survey on Transfer Learning," IEEE Transactions on Knowledge and Data Engineering, vol. 22, no. 10, pp. 1345–1359, 2010.

[20] A. Ghosh and L. C. Jain, Evolutionary Computation in Data Mining. Studies in Fuzziness and Soft Computing, Springer Berlin Heidelberg, 2006

[21] Boualouache, A.; Senouci, S.M.; Moussaoui, S. A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks. IEEE Commun. Surv. Tutor. 2018, 20, 770–790.

[22] Raya, M.; Hubaux, J.P.; Ning, P.; Du, W. Securing vehicular ad hoc networks. J. Comput. Secur. 2007, 15, 39–68.

[23] Artail, H.; Abbani, N. A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks.IEEE Trans. Dependable Secur.Comput. 2016, 13, 106–119.

[24] Boualouache, A.; Moussaoui, S. S2si: A practical pseudonym changing strategy for location privacy in vanets. In Proceedings of the 2014 International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, Algeria, 17–19 June 2014; pp. 70–75.

[25] Wu, F.; Xu, L.; Kumari, S.; Li, X. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security. J. Ambient Intell. Humaniz.Comput. 2017, 8, 101–116.

[26] Jiang, Q.; Ma, J.; Wei, F.; Tian, Y.; Shen, J.; Yang, Y. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. J. Netw. Comput. Appl. 2016, 76, 37–48.

[27] Arafin, M.T. Hardware-Based Authentication for the Internet of Things. Ph.D. Thesis, University of Maryland, College Park, MD, USA, 2018.

[28] Vaidya, B.; Makrakis, D.; Mouftah, H. Two-factor mutual authentication with key agreement in wireless sensor networks. Secur.Commun.Netw. 2016, 9, 171–183. Electronics 2023, 12, 1812 19 of 21

[29] Hu, H.; Liao, L.; Zhao, J. Secure Authentication and Key Agreement Protocol for Cloud-Assisted Industrial Internet of Things. Electronics 2022, 11, 1652.

[30] Mishra, D.; Vijayakumar, P.; Sureshkumar, V.; Amin, R.; Islam, S.H.; Gope, P. Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimed. Tools Appl. 2018, 77, 18295–18325.

[31] Chang, I.P.; Lee, T.F.; Lin, T.H.; Liu, C.M. Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks. Sensors 2015, 15, 29841–29854.

[32] Dolev, D.; Yao, A.C. On the security of public key protocols. Inf. Theory IEEE Trans. 1981, 29, 198–208.

[33] Xue, K.; Meng, W.; Li, S.; Wei, D.S.; Zhou, H.; Yu, N. A secure and efficient access and handover authentication protocol for Internet of Things in space information networks. IEEE Internet Things J. 2019, 6, 5485–5499.

[34] El-Meniawy, N.; Rizk, M.R.; Ahmed, M.A.; Saleh, M. An Authentication Protocol for the Medical Internet of Things.Symmetry 2022, 14, 1483.

[35] Tewari, A.; Gupta, B.B. A novel ECC-based lightweight authentication protocol for internet of things devices. Int. J. High Perform. Comput.Netw. 2019, 15, 106–120.

[36] Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J.J. Cloud centric authentication for wearable healthcare monitoring system. IEEE Trans. Dependable Secur.Comput. 2018, 17, 942–956.

[37] Gupta, M.; Gupta, K.K.; Shukla, P.K. Session key based novel lightweight image encryption algorithm using a hybrid of Chebyshev chaotic map and crossover. Multimed. Tools Appl. 2021, 80, 33843–33863.

[38] Liu, L.; Jiang, D.; Wang, X.; Rong, X.; Zhang, R. 2D Logistic-Adjusted-Chebyshev map for visual color image encryption. J. Inf. Secur. Appl. 2021, 60, 102854.

[39] Sun, J.; Zhao, G.; Li, X. An improved public key encryption algorithm based on Chebyshev polynomials. Indones. J. Electr.Eng. Comput. Sci. 2013, 11, 864–870.

[40] Zhang, L. Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals 2008, 37, 669–674.

[41] Srinivas, J.; Das, A.K.; Wazid, M.; Kumar, N. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things. IEEE Trans. Dependable Secur. Comput. 2018, 17, 1133–1146.

[42] Sarkar, A.; Singh, B.K. A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimed. Tools Appl. 2020, 79, 27721–27776.

[43] Rui, Z.; Yan, Z. A survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE Access 2018, 7, 5994–6009

[44] Griffin, P.H. Secure authentication on the Internet of Things. In Proceedings of the SoutheastCon 2017, Concord, NC, USA, 30 March–2 April 2017; pp. 1–5.

[45] Mayron, L.M. Biometric authentication on mobile devices. IEEE Secur. Priv. 2015, 13, 70–73.

[46] Neal, T.J.; Woodard, D.L. Surveying biometric authentication for mobile device security. J. Pattern Recognit. Res. 2016, 11, 74–110.

[47] Bureva, V.; Sotirova, E.; Bozov, H. Generalized Net Model of Biometric Identification Process. In Proceedings of the 2018 20th International Symposium on Electrical Apparatus and Technologies (SIELA), Bourgas, Bulgaria, 3–6 June2018; pp. 1–4.

[48] Dharma Putra, G.; Kang, C.; Kanhere, S.S.; Won-Ki Hong, J. DeTRM: Decentralised Trust and Reputation Management for Blockchain-based Supply Chains. In Proceedings of the 2022 IEEE International Conference onBlockchain and Cryptocurrency (ICBC), Shanghai, China, 2–5 May 2022; pp. 1–5.

[49] Song, Y.; Sun, C.; Peng, Y.; Zeng, Y.; Sun, B. Research on Multidimensional Trust Evaluation Mechanism of FinTech Based on Blockchain. IEEE Access 2022, 10, 57025–57036.

[50] Jeribi, F.; Amin, R.; Alhameed, M.; Tahir, A. An Efficient Trust Management Technique Using ID3 Algorithm With .Blockchain in Smart Buildings IoT. IEEE Access 2023, 11, 8136–8149