**Artificial Intelligence of Things(AIoT)**

**Ms Priyanka Nanda**

**School of Computational Science**

**GNA University, Punjab, India**

**ABSTRACT**

With this emerging trend of Computer Science, new technologies have been developed with new evolution. Internet of things is the best way to communicate with devices with their unique features. Internet of things (IoT) is the newer technology which associated with different devices and objects. Here we have to mention chapter 1includes the introduction about the Artificial Intelligence IoT, importance of Artificial Intelligence IoT, Benefits of AIoT Systems, How AI is changing IoT, IoT Vs Sensor Networks, **Artificial Intelligence IoT in secure and efficient authentication.**

Keywords: AIoT, Sensor Networks, Aerial Networks, Traffic management, Machine Learning.

1. **Introduction**

Artificial intelligence of things (AIoT) is the mixture of artificial intelligence (AI) technologies and the internet of things (IoT) infrastructure. AIoT's goal is to create more structured IoT operations, improve human-machine interactions and strengthen data management and analytics.

AI is the replication of human intelligence processes by machines, especially computer systems, and is typically used in natural language processing, speech recognition and machine vision.

IoT is a system of associated computing devices, mechanical and digital machines or objects with distinctive identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. A thing in IoT can be a person's heart monitor implant, an automobile with built-in sensors to alert the driver when tire pressure is low, or any other object that can be assigned an Internet Protocol address and transfer data over a network.

AIoT is reframing and commonly beneficial for both types of technology, as AI adds value to IoT through machine learning capabilities and upgraded decision-making progressions, while IoT adds value to AI through connectivity, beckoning and data exchange. AIoT can improve businesses and their services by screating more value out of IoT-generated data. AI enables the IoT device to use gathered big data to better analyze, learn and make decisions without the need for a human.

**+ =** People-oriented IoT

AIoT

IoT

AI

**figure 1.1: 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. In modern years, sensors connected to IoT are already being used to handle lighting, supplies, air conditioning, access, among others. In grouping with AI algorithms, energy management and efficiency plans can be recognized, creating more comfortable and safer environments for humans as well as sustainable ones. Following are the different applications where AIoT is used:

1.1.1. Smart Cities: In a Smart City, it is possible to centrally control areas and services of the city such as traffic, transport, charging points, waste management, lighting, parking areas or environmental quality, among many others. The sensors, placed in each area or service, send data through IoT, which are collected and processed with Artificial Intelligence, establishing patterns and trends that, after analysis, allow predicting and/or anticipating future flows and demands, allowing cities to be more efficient and reduce environmental impact.

1.1.2. Smart Industry: In Smart Industry, the possibilities are much broader. Some of the benefits of implementing an AIoT system include: greater efficiency, higher productivity, resource savings and even decrease of CO2 emissions. Moreover, this technology does not differentiate against any sector and can be used by all types of companies, from SMEs to multinational industries. IoT systems interconnected in real time generate large amounts of data, which can be processed and analyzed by AI algorithms, converting them into valuable information, allowing managers and middle management to make better decisions based on more accurate data.

1.1.3. Smart Traffic: A congested road is inconvenient on many levels. It means longer waiting hours, loss of gas, and increased emissions. The road is a crucial factor for every logistics company. Without reliable information, the truck drivers may end up in a long build-up on a busy highway. So to increased the efficiency, it would be more important to use AIoT in smart traffic. In smart traffic, embedded system in an IoT ecosystem has become so robust that they assess traffic patterns, weather, and other factors to solve real-world problems. Companies can now use embedded software to tackle traffic congestion once and for all

1. **Benefits of AIoT Systems in Traffic Management**

AIoT empower road safety by drumming into a wide range of earlier unavailable data. Following are various benefits of this system:

1. Collection of traffic counts and real-time relay
2. Decreased wait time at signals and on highways
3. Proactive traffic management despite dynamic conditions
4. Striking the right balance between traffic density
5. Reduction in carbon monoxide emissions
6. Increasing road safety as this system leaves minimal margin for error

High scalability scalabiliy

Benefits of AIoT

Enhanced products & services

Improved operational efficiency

Avoids unplannedd

Costly downtime

Better risk management

**figure 2.1: Benefits of AIoT**

1. **Impact of AI on IoT**

Over the past few decades, the business world has seen steady adoption of the Internet of Things (IoT). The next brandish of IoT evolution is leading us as advances in Artificial Intelligence (AI) and Machine Learning(ML) keep under control the possibilities of IoT devices utilizing “Artificial Intelligence of Things,” or AIoT. AI is changing IoT by making it easier for humans to interact with devices.The IoT is changing the face of technology with its interconnected devices data collection and analysis. Artificial Intelligence (AI) and Machine Learning (ML) are the two key technologies that gives IoT a boost in terms of user experience system responsiveness and automation.

Artificial Intelligence (AI) enables machines to learn how to perform tasks based on new data inputs. Machine Learning (ML) makes it possible for computers to analyse data quicker and spot patternsfor future predictions. Both artificial intelligence (AI) and machine learning (ML) have gives a massive boost to different industries including healthcare retail, logistics, finance, agriculture, etc. Artificial Intelligence is a technology that is capable of improving device performance. However, IoT devices do not need to be as complex as a computer to benefit from AI. Due to the connected nature of IoT, the use of AI can be extended in various ways. One such way is helping IoT devices understand human communication.

For example: if you are using a remote controller to turn on the air conditioner, the air conditioner device will understand your language. That’s because the device is capable understanding human language through the use of AI. Therefore, you don’t have to press different buttons to adjust the air conditioner. You can simply use voice commands to adjust the temperature of the room. Since IoT devices are connected to each other and to the internet, they can collect aIoT data. It has different data on sensors which can be better use with the help of Artificial Intelligence. For this reason, it can be used in IoT devices to make devices more smart and more efficient. It can also raise the productivity and efficiency of IoT devices by a large fraction. It can be used to respond human commands and also to perform tasks autonomously.

1. **IoT Vs Sensor Networks**

Wireless sensor network (WSN) is a collection of independent devices that create an ad hoc network to gather information from the physical environment. It consists of a cluster of sensor networks; field area networks (FANs), mesh networks, narrowband IoT (NB-IoT), and body area networks (BANs). These appliances are low-powered and send data via specific communication protocols. IoT systems are instigated to collect and evaluate data from each of these independently linked devices. Public cloud providers provide storage and apps, whereas private cloud providers give such services to a limited number of customers.

One example of a WSN is a network of sensors on a boat’s hull to detect water intrusion. Each sensor has a unique ID and functions independently from the other sensors in this case. Each sensor is typically battery-powered and uses an ultralow-power protocol to send information to a central gateway. The gateway processes collective all the data collected from the sensors before sending it to the IoT platform. Another example of a WSN is a network of nodes used in infrastructure management. They have made people’s lives more suitable and effective.

Wireless Sensor Network

Glass break sensor

Window open sensor

Door Open Sensor

Motion Detector

Security Camera

**figure 4.1:Wireless Sensor Network**

Internet of Things(IoT)is aThe IoT (Internet of Things) describes the network of physical objects that are enclosed with sensors, software, and other technologies to connect and reciprocate data with other devices and systems over the internet.  The term IoT markedly improves the approach which can control and monitors all the processes taking place in our homes. The IoT-based home security system allows users to monitor and manage the security of their home including door access and surveillance. Intelligent home systems provide efficient energy with the use of smart lighting, intelligent home systems require the use of intelligent algorithms that gives household devices a certain level of autonomy. We have parameters to compute energy so that it makes communication and collaboration with smart objects. For improvement, we have to propose a hybrid Intruder detection system and edge computing. We propose an automatic, secure, energy-efficient, cost-effective, and reliablesolution to the smart home based on edge computing functionality. Using IoT-based home automation, we have to control the sound, and lighting system and automatically switch on/off the fan using sensors. Home automation refers to the capacity to use internet-connected tools to operate household appliances.

Along with home automation, we have to use home security systems where we ensured the protection of our homes. The IoT-based home security system allows users to monitor and manage the security of their home including door access and surveillance. The owner can also capture the image of the intruder who is trying to access the door. The door will open once the correct person is recognized using sensors.

Intelligent home systems also provide efficient energy with the use of smart lighting, it also requires the use of intelligent algorithms that give household devices a certain level of autonomy. We have different parameters to compute energy so that it makes inter-network communication and collaboration with smart objects possible. For improvements, we have proposed Hybrid IDS and Edge Computing. Hybrid IDS consists of anomaly and misuse detection modules. It is more effective to detect and respond to cyber-physical attacks in DER Systems.

### Table 1: IoT vs. Wireless Sensor Network

|  |  |  |
| --- | --- | --- |
| **Basis** | **IoT** | **Wireless Sensor Network** |
| Architecture | IOT has a gateway that can connect to internetworks (having routers, switches, APs, etc.). | WSN consists of a network of only sensors |
| Devices | IOT runs IPv6 in the sensor network (802.15.4 MAC/PHY) and IPv4 on the internetwork portion. | WSN runs IPv4 and features a sink (not a gateway) |
| Protocols | Routing protocols in NetSimIoT include AODV and RPL. | Routing protocols in NetSim WSN include DSR, AODV, OLSR, and ZRP. |

1. **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, the extension of space-time coverage leads to numerous theoretical and technical challenges with respect to the development of space information networks given the restricted spectrum, energy, and orbit resources.

5.1 Difference between Conventional and Wireless Communication Systems

**Wired / Wireless**

Conventional and wireless are the two different systems used for communication. A very notable difference is the presence of wire in the conventional communication system. The techniques used in both systems infra structure are same such as core elements of the network services. A wired network communicates through wires while wireless communication systems utilize radio waves.

**Complicated / Non-complicated**

Conventional wired communication system is uncomplicated to install and fix but wireless communication system is complicated to establish. Its maintenance and troubleshooting are not possible without expert.

**Mobility / immobility**

Immobility is the bigger flaw of wired communication system as it makes you reluctant to not to leave your place in any condition. Wireless communication system gives you the ease of mobility and u can sit wherever you want while doing your work.

**Costly / Cheap**

An additional cost in the form of wires and cables is attached with the wired system and makes the budget heavy while wireless communication has no issue of cabling and the price is very affordable.

**Speed**: The transmission speed of the wired network has given it an edge over wireless system. In wired system, there is no need of sharing space and therefore no user interface. Wireless communication system has to share it band with sometimes multiple users that may reduce the transmission speed.

**Seen / Unseen**

Wireless system makes you excite to do uncertain thing like it transmit data (command to play n share music, print the document, and sharing of files) unseeingly with the help of radio waves. Other examples of the wireless communication system are Bluetooth and cordless phones, etc.

**Reliability**

Conventional communication systems as wired or Ethernet are coming in most powerful form as they promise to give you good speed nearly 1000 Mb/s that is faster than previous and all other Types of connections plus enhanced security as well. Further it is not a big deal to get high speed and security at reasonable price. Hence a wired system is more reliable than wireless.

**Home Users / Corporate Users**

Wireless network could be a good choice for home users as it works better and speed is not a big issue. In an office environment, however, wired communication system is preferred as there is need of high speed data transmission and security. However, as the offices are becoming mobile so there is demand for wireless system to take portable data. There is no such fuss in case of wireless system as downtime that is an issue in wired system. Wireless system is easy to install as Wireless USB helps you to connect in few moments. To change the place of a system in office just takes the system to the desired place with the card.

**Hotspot**

Hotspot is becoming a popular term associated with wireless system. Internet is provided to the user as a promotional package by the owner in public places, libraries, hotels, schools, airports, railway stations to facilitate the users with it and entice them as well. In case of wired network you have internet access only through wire, there is no concept of hotspot.

**Quality of  Service (QoS)**

A negative point of wireless communication is the quality of service (QoS). It has no surety to have constant receiving of powerful signals as environmental changes and other hindrances (walls, birds or planes) may interrupt the signals.

**Virtual Network**

A positive point of wireless communication is in the form of WLAN as it makes virtual network by the users in its vicinity like university or library. It provides them wireless internet access. There is no need of access point to be connected with the internet.

5.2 Non-Conventional methods of communication

Following are the different ways to communicate:

* Visual Art
* Music
* Letters
* Tactile Communication
* Sports and Games

### 5.2.1 Visual Art

Words, written or spoken, are not always the best way to converse. Art can be a fantastic alternative. Drawing pictures, painting or sculpting can be a better way to communicate. After all, a picture is worth a thousand words. Showing an artistic creation can get a point across more quickly, and more powerfully, than a box of text. This is why billboards and magazine ads are such a long-standing form of marketing, and why logos dominate everyday life. The classic Golden Arches of McDonald’s or white swoop of Nike instantly conjure positive memories and responses in consumers of all ages.

### 5.2.2 Music

Sounds can communicate just as well as visual art. Music is an accessible form of communication that anyone can use. Written music can be read across cultures and continents. Music can express anger, happiness, peace or sorrow. According to the Mayo Clinic music can even overcome dementia. Musical therapy can improve quality of life for patients with dementia because it triggers deeply held feelings of joy.

### 5.2.3 Letters

Old-fashioned, “snail mail” letters used to be one of the most important methods of communication. In the Internet age, hand-written letters aren’t as popular. This creates a unique opportunity for memorable communications. Writing a letter or note by hand shows a deliberate, personal effort. Letters also offer room for creativity. They can be written on personalized stationery, illustrated with drawings or penned in multiple colors of ink. The tactile experience of opening a letter and seeing bright, beautiful colors popping off the page brings happiness to readers. According to Entrepreneur.com, a handwritten letter can even increase customer relations.

### 5.2.4. Tactile communication

It doesn’t take a communications degree to understand that tactile experiences are tied to memories. Still, using touch is an often overlooked form of communication. This method of communicating takes many forms: Tapping a shoulder instead of shouting for attention, picking up the desired shopping item instead of pointing at it or holding someone’s hand. Tactile communication is a simple but effective method, and it can lead to improved retention of new ideas — or shopping lists.

### 5.2. 5 Sports and Games

Sporting is so popular in American culture it’s spawned a unique degree: A bachelor’s in sports communication. Sports are used to build social skills with youth teams, create a better environment in the office or simply bring people together in front of the TV. Games are another growing hobby, with more people than ever playing video games and board games.

**VI Artificial Intelligence IoT in secure and efficient authentication**

With fast-evolving cyber attacks and the rapid multiplication of devices taking place currently, AI and machine learning can help to keep abreast of cybercriminals, automate threat detection, and respond more effectively than conventional software-driven or manual techniques. Security and authentication will continue to improve and become smarter. Eventually, authentication will likely move from supervised learning, where the dataset includes the outcomes, to unsupervised learning where AI finds new patterns that humans may not have discovered and makes predictions of potential factors to assess. Being able to cross reference multiple machine learning algorithms and use pattern recognition and time-series based predictive algorithms will improve the accuracy and scope of AI-based authentication offerings going forward, for web application logins, but also for other aspects of cybersecurity such as network intrusion and botnet detection. AI develops more effective algorithms to determine which factors indicate an attack by trying different techniques to solve problems and checking its answer against the answer in the dataset. Eventually, it finds a set of algorithms that enable it to accurately predict threats most of the time.

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

* Artificial intelligence in secure and efficient privacy preserving set intersection with identity authentication in IoT
* Artificial intelligence in efficient privacy preserving anonymous authentication scheme for human predictive online education system
* AI in quantum secure authentication and key agreement multi agent interaction for public cloud
* Secure data sharing algorithm in privacy protection for IoT public cloud
* AI in efficient authenticated group key agreement protocol for dynamic UAV fleets in untrusted environments.

6.1 Authentication and authorization

Authentication is the process of device identification, while authorization provides permissions. IoT devices use these processes to do role-based access control and ensure that devices only have access and permission to do exactly what they need. Only authorized devices can interact with other devices, applications, cloud accounts and gateways.

Administrators register each device when they deploy it on the system. The system validates devices when they connect and share data. Many organizations use public key infrastructure (PKI) to link devices with public key certificates from certificate authorities to assign and verify device identities. PKI establishes an IoT device's legitimacy on a network to share data.

6.2 Authentication and Authorization models and Types

There are two types of models:

* Distributed Model
* Centralized Model

6.2.1 Distributed Model

The distributed model defines a way of contact in between the components of a system and it refers to how resources are spread out and works on more than one device to improve the effectiveness and performance of a task.

The distributed models are used in many areas; some are:

• Distributed database model – It specifies that the storage is not attached in a single common processor; it may store in many computers which may be located in different locations.

• Distributed network model – It specifies that the networking system is spread out for the computer program and the data across more than one computer that make use of low cost computer [power](https://www.chegg.com/learn/mechanical-engineering/heat-transfer-thermodynamics/power) and operate the data more efficiently with a mix of desktops.

• Distributed computing model – It specifies to share the component of a [software](https://www.chegg.com/learn/computer-science/computer-technology/software) system in a distributed manner to improve the efficiency and recital.

Problems on designing a distributed model.

• Usage of widely varying modes.

• Wide [range](https://www.chegg.com/learn/statistics/introduction-to-statistics/range) of system environments.

• Internal problem and external threads.

Distributed Model is also known as mutual authentication, this protocol is used when both devices authenticate each other before they communicate. Each device must have a exceptional digital identity stored for the other device and then compare identities. The devices can only connect when the first device beliefs the second device's digital certificate and vice versa. The Transport Layer Security protocol exchanges and compares certifications.

6.2.2 Centralized Model

Centralized Model tells the strategic planning, goal setting, budgeting, and talent deployment are typically conducted by a single, senior leader or leadership team. In contrast, in decentralized organizations, formal decision-making power is distributed across multiple individuals or teams. In centralized model, it is used to focus by placing power and authority in a center or central organization. centralized several functions in a single agency.

In the authentication model of centralized, an admin registers the devices with a central authority or server and connects the devices with valid digital certificates. The central authority simplifies the secure handshake between the two devices that wish to communicate. In three-way authentication, the security certificates aren't stored on the devices and can't be stolen by criminals, yet the devices still have strong security.

This methodology works best for always-connected devices or ones with on-demand internet access because it eliminates any authentication delay. A certificate and key lifecycle management service can manage the certificates centrally and connect to any device on a network that needs verification.

**Reference**

[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,” Acta Informatica, 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 June

2018; 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 on

Blockchain 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