Using disruptive technologies as blockchain and AI in IoT cybersecurity

Ivan Gaidarski
Unmanned Robotic Systems Lab
Institute of Robotics "St. Ap. and Gospeller Matthew"
Bulgarian Academy of Sciences
Sofia, Bulgaria
ivangaidarski@ir.bas.bg

Abstract - **In this article, we examine innovative methods for ensuring cybersecurity of the Internet of Things (IoT) infrastructure. These methods are based on new revolutionary technologies such as artificial intelligence and blockchain. We examine aspects such as the architecture of IoT, typical vulnerabilities and attacks against IoT, classic methods for protecting data, communications and devices in the Internet of Things (IoT). We also examine the essence of new revolutionary technologies such as blockchain and AI and their application for ensuring IoT cybersecurity.**

Keywords: IoT, AI, artificial, intelligence, blockchain, disruptive, cybersecurity, attack, protection

I. Introduction

The term “Internet of Things” (IoT) refers to networked electronic and physical devices, sensors and actuators. IoT communicate and exchange data with each other and, through networks such as the Internet, transmit data to the corresponding control and computing devices.

Their exponentially growing number, as well as the critical importance of IoT in various aspects of modern life, require ensuring the security of the IoT ecosystem. As IoT is inextricably linked to communication in the Internet environment, we are talking about cybersecurity of the IoT infrastructure.

In this article, we examine some innovative and disruptive methods for ensuring cybersecurity of the Internet of Things (IoT). These methods are based on new revolutionary technologies such as artificial intelligence and blockchain. We examine aspects such as vulnerabilities and attacks against IoT, methods for protecting data, communications and devices in the Internet of Things (IoT).

II. IoT ecosystem

By definition, Internet of Things (IoT) devices are defined as physical objects connected to the Internet and capable of collecting and exchanging data. These objects can be physical devices such as vehicles, sensors, relays, actuators (on/off keys, valves, switches, actuators, interrupters), electronic devices (controllers, fans, thermostats, trackers, heaters, coolers), computing machines (cloud and edge computers, mobile computers, Raspberry PI). The communication itself can be carried out over various protocols and transmission networks, between people, people-devices or devices-devices.

The versatile use of IoT devices in everyday life and business for the purposes of industrial production, communication, healthcare, education, sports and many other activities is the reason for the sharp in their number. In 2025, the number of IoT devices will reach 20.1 billion worldwide,

which is an increase of 13.21% compared to 2024 [1].

This growth of IoT is driven by enterprise adoption, digital transformation, and the increasing integration of IoT with artificial intelligence, 5G, and edge computing, such as the Industrial IoT (IIoT) sector.

The vast number of connected IoT devices is building a communication infrastructure that has the potential to grow into a self-contained next-generation communication network [2]. These interconnected IoT devices are used in a number of areas such as:

1. Smart Home,
2. Healthcare,
3. IoT Automotive,
4. Logistics,
5. Smart Agriculture,
6. Smart Energy Distribution,
7. Retail sector,
8. Wearables,
9. Entertainment,
10. Education,
11. Smart Cities,
12. Industrial IoT.

Smart Home

The purpose of IoT devices in this category is to manage security systems, video surveillance, air conditioning, ventilation, lighting, utilities and home appliances. The main role of IoT devices is monitoring and management without human intervention, including remotely. There are no high requirements for communication speed, only for a reliable connection. A large part of IoT activity is automated. There are low requirements for computing resources, but high requirements for security, privacy and reliability.

Healthcare

In the field of healthcare, the role of IoT is monitoring various health parameters, supporting diagnostic, therapeutic and rehabilitation activities, alerting and supporting medical or emergency assistance when necessary. This area also includes medical robots such as Da Vinci Robotic Surgical Systems. The requirements for IoT infrastructure are very high, due to the fact that critical activities for human health and life are performed. There are high requirements for fast, stable and reliable communication, providing backup power to critical

ACKNOWLEDGE THE FINANCIAL SUPPORT OF THE PROJECT WITH FINANCING AGREEMENT NO. PVU-44 OF 05.12.2024 UNDER PROJECT NO. BG-RRP-2.017-0011 "ECOLOGICAL COLLABORATIVE ROBOTS POWERED BY GREEN HYDROGEN" UNDER THE RECOVERY AND RESILIENCE MECHANISM FOR THE IMPLEMENTATION OF AN INVESTMENT UNDER C2I2 "INCREASING THE INNOVATION CAPACITY OF THE BULGARIAN ACADEMY OF SCIENCES (BAS) IN THE FIELD OF GREEN AND DIGITAL TECHNOLOGIES" FROM THE RECOVERY AND RESILIENCE PLAN, BULGARIA.

components and duplication of main nodes. Other important requirements are for cyber-security and privacy. It can be considered as part of Smart Home and Smart Cities. AI is widely used in this area of IoT [4].

IoT Automotive and Logistics
The goal of IoT systems in the field of Automotive and Logistics is to achieve increasingly higher autonomy of transport, including self-driving cars and robotic vehicles. The future goals of this area also include the development of autonomous diagnostics, as well as autonomous and remote repair activities. Here, the requirements for the infrastructure parameters are high - high communication speeds, reliability and wide coverage. The requirements for reliability and security are extremely high, mainly for safety purposes. This part of IoT is also characterized by high requirements for the quality of IoT devices. An example is the fact that modern cars contain over 100 sensors, with a tendency to increase.

Smart Agriculture
In the field of smart agriculture, the main requirements for IoT are the collection, processing and communication of large amounts of data needed for GIS, crop monitoring, soil moisture, fertilization management, management of various facilities and vehicles, objective control, weather and natural disaster prediction. The requirements for the infrastructure are for a wide range of communication coverage and increased requirements for computing power due to the need to process huge amounts of data. This area also includes functions such as animal tracking, health monitoring, food, fodder and waste management.

Smart Energy Distribution
The role of IoT systems is to monitor, measure and control the production, transmission and distribution of energy to end users, billing and maintenance of the electricity grid. The requirements for the system are very high, due to the central role of energy for the normal life of people and industry as well as for all other types of IoT systems.

Retail
This area includes supply management, logistics, sales, warranty service and intelligent inventory management. There are no high requirements for the infrastructure, except for reliability and safety.

Wearables
This includes various smart gadgets as watches, fitness trackers and sensors for measuring health indicators. There are also no high requirements for infrastructure. The requirements for safety and privacy are increased.

Entertainment and Gaming
IoT devices in this category are related to Games, Virtual Reality (VR) and Augmented Reality (AR). An area with high potential for expansion. There are no high requirements for IoT infrastructure, except for sensor precision and ensuring safety and privacy.

Education
A very promising area related to Smart Education, Smart classroom and STEM centers. High requirements related to ensuring safety and privacy.

Smart Cities
Here the role of IoT devices is more complex. The goal is to manage entire areas of modern city life such as street traffic, utilities (water, gas, sewage) on a city and surrounding scale, retail sector, healthcare, air quality control, waste management, street lighting and video surveillance, etc. Here there are increased requirements for security, low latency of communications, high availability and reliability and very high requirements for scalability and flexibility of IoT systems.

Industrial IoT
Industrial IoT (IIoT) encompasses the management of intelligent industrial assets - resource and material management, production, supply chains, logistics, customer relationships, service. Technologies such as Cloud, Edge and Fog computing, AI and Big data analytics are strongly present in this area. It is characterized by high requirements for the quality of IoT devices and IoT infrastructure - reliability, speed and coverage. There are also high requirements for computing power, due to the processing and analysis of large amounts of data. There are particularly high requirements for ensuring high levels of cybersecurity, privacy and reliability. This area largely includes elements from other IoT segments.

From a security perspective, among the many IoT use cases, we can distinguish 2 special cases - massive IoT and mission critical IoT.

Massive IoT. In the first case, we have a large number of IoT devices that transmit small amounts of sensitive data. Such are, for example, devices that are part of Smart Home or Smart Agriculture. The data that is transmitted from IoT devices to the cloud or to the receiving station is not large in volume and does not require high speed, but on the other hand, it requires wide signal coverage and a stable connection.

In **mission critical IoT**, due to the specifics of the activity, we have increased requirements for connection reliability and low network latency [3].

Since IoT is a network of interconnected heterogeneous objects, a flexible architecture is needed, allowing both seamless communication and easy expansion by adding or removing new devices. So far, there is no consensus established common reference model, but it can be assumed that the basic architecture of IoT is based on the three-layer model shown in Fig.1 [3].

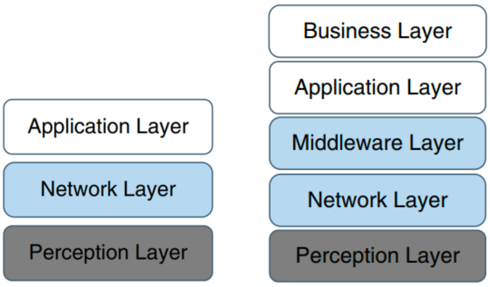

Fig. 1. Three-layer and Five-layer architectures

The first layer, called the "Perception layer", performs the interaction with external physical objects. It consists of various devices such as sensors, actuators and control devices for collecting data and manipulating various parameters through the executive devices. The collected information is transmitted to the next layers.

The next layer - "Network layer" provides the network infrastructure and protocols for data transmission between the different layers, respectively IoT devices and computing and storage resources, be they cloud, local or remotely located. It consists of various communication devices (mobile networks, Bluetooth, Wi-Fi), network devices (routers and gateways) and provides communication through specific protocols such as Bluetooth, Zigbee (IEEE 802.15.4), DSRC (IEEE 802.11p), Ethernet, Wi-Fi, Z-Wave, LPWAN, VSAT, NFC, Li-Fi, RFID, LTE, 5G, etc.

The "Application layer" provides interaction with users and controlled assets through various applications in which the received data is processed and decisions are made based on the respective goals. This layer provides the main functionality of the various areas of the IoT ecosystem - Industrial IoT, Smart Cities, Smart Agriculture, Healthcare and etc.

Recently, a five-layer model has also gained popularity, with 2 new layers added to the three-layer model shown - Business and MiddleWare layer. The Business layer adds a higher level of services in the various areas of the IoT ecosystem, using business models and behavior patterns and ensuring the completeness of services, including billing and service services. The MiddleWare layer takes care of the processing and storage of information from the Network layer to the Application layer, using various computational libraries, connection to databases, etc.

III. THREATS TO IOT

The ever-widening application of IoT devices, as well as the sharp increase in their number and areas of use, also expands the surface of vulnerabilities from cyber-attacks, insider threats and privacy threats.

Since security is not a priority at the core of IoT device design, it is necessary to compensate for this by designing cyber-resilient IoT systems, including the devices themselves, communication devices, channels and protocols, computing resources, and the use and distribution of raw, intermediate, and final data. Other factors affecting IoT security are the lack of uniform standards in the production of IoT devices, the lack of regular device firmware updates, the lack or non-compliance with password change policies, etc.

IoT is essentially a large-scale heterogeneous network connecting different heterogeneous objects, and integrating different communication protocols, cloud services, heterogeneous data with different characteristics. They can be considered as a complex IT system. To study the threats to it, we use the model shown in Fig. 2, showing the basic concepts of the "Cybersecurity" perspective to the system.

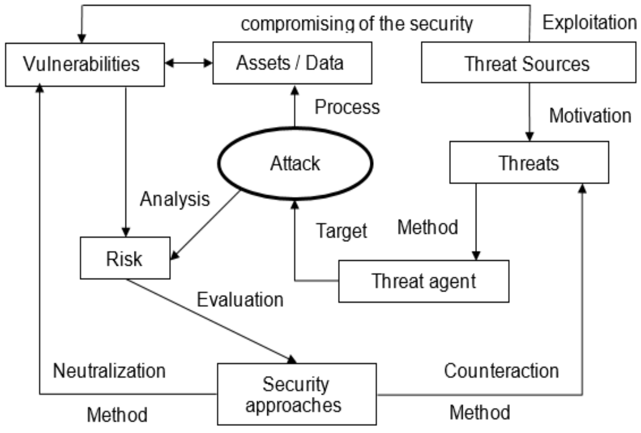

Fig. 2. Basic concepts of CyberSecurity perpective

Attacks on IoT infrastructure are no different from attacks on standard IT infrastructure, communications, and services. The difference is in scale - with IoT we have vast number of devices and communication channels. The essential difference between the two types of infrastructure is the low level of protection of IoT by default.

We examine some unique characteristics of the IoT environment compared to standard IT infrastructure:

- IoT devices are diverse in type, functionality, hardware architecture and operating systems,
- There are no generally accepted industry standards, manufacturers use their own hardware solutions,
- They are seriously limited in terms of their own resources in terms of computing power and storage capacity,
- Due to their vast number, IoT devices generate a huge amount of data, which has a different structure and storage formats,
- The data itself is stored locally, on servers or in the cloud

These features also determine the measures for detecting, suppressing and combating threats to the IoT environment.

To analyze the various vulnerabilities, attacks and countermeasures against them, we will use the three-layer model of IoT architecture - Fig3[3].

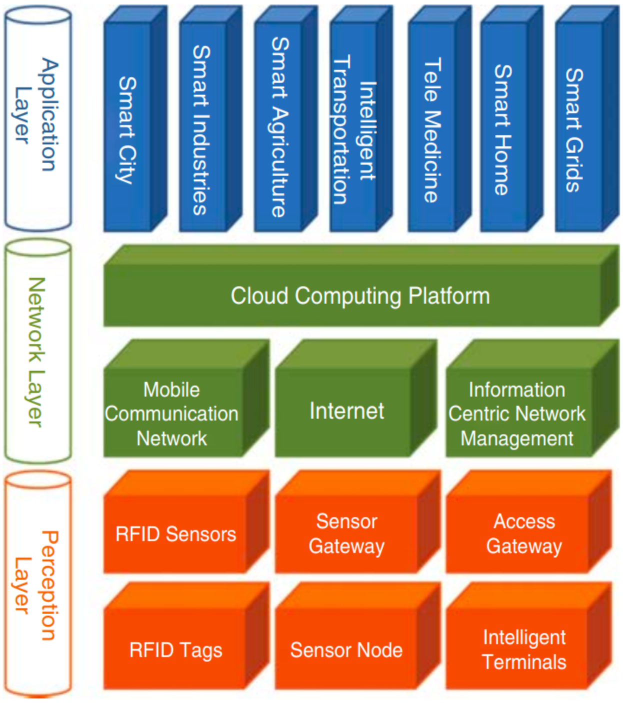

Fig. 3. Entities of the three-layer architecture

The objects and services associated with the corresponding layers - Perception, Network and Application layers use different technologies, communication protocols, different data types and functionalities. This fact enormously expands the vulnerable surface of the IoT infrastructure, respectively the damage from successful attacks and complicates the effective action of the corresponding countermeasures.

In Table 1 we consider some of the typical attacks and countermeasures to the corresponding layers and their elements.

TABLE I. ATTACKS AND MEASURES TO IOT

Layer Entity		Attacks	Measures
Perception	RFID Tags	Spoofing, Eavesdropping, Tracking, DoS, DDos, Repudiation	Access control, Hash-based AC, Data and Channel Encryption, IPSec protocol, Ciphertext Cryptography for side channel attack, Hidden Communication
	Sensor Nodes	Physical attacks, Node Outage, Impersonation,, Tampering, Jamming, Information gathering, Message interception, Subversion,	Sensor Privacy, Authentication
	Sensor Gateway	DoS, Interception, Man-in-the-middle MiM Interruption, Modification, Misconfiguration, Fabrication	Device Security, Message Security, Integrations Security
Network	Internet	DoS, DDoS, Hacking, Identity theft, Cyberbullying, Viruses, Loss of Integrity and Confidentiality	Identity Management, Communications Encryption PKI based secure channels
	Mobile	DoS, DDos, Eavesdropping, Tracking, Bluesnarfing, Bluejacking, Bluebugging, Corruption, Deletion	Secure access control - Biometrics, Time changing session keys, Public-key crypto primitives
	Cloud	Physical security, Infrastructure security Encryption, System complexity, Data access controls, Identity management, Misconfiguration of software	Pseudo anonymisation, Connection anonymization Trapdoor permutation Secret sharing Cryptographic One-way hash chain Zero knowledge proof Aggregated transmission evidence
Application	Smart Home, Industy, Agri-culture, Helath, Energy	Access control, Tampering, Code injection, Disclosure of information, Data Leakage	Authentication, Information Flow Control Datagram Transport Layer Security (DTLS) End-to-end encryption Key agreement Data Leak Prevention DLP

The layers and their entities in the IoT architecture use different specific technologies and protocols for data communication, associated with specific vulnerabilities and protection measures. Classic protection measures such as access control, authentication and identification, encryption of channels and data, regular updates of hardware IoT components and communication devices are not effective due to the peculiarities of the IoT infrastructure. For this purpose, entirely new technologies must be used, which, combined with traditional protection methods, can achieve a drastic jump in the effectiveness of protection against the new sophisticated threats.

IV. NEW DISRUPTIVE TECHNOLOGIES FOR IOT PROTECTION

We look at new technologies like Blockchain (BC) and AI. These technologies have the potential to take the security of the Internet of Things to a new level, so that it can respond to new threats and challenges to data security and privacy.

A. Blockchain

The blockchain is a peer-to-peer distributed ledger with online records to ensure trusted transactions without the intervention of a third party. Blockchain technology records all transactions made online without allowing any exceptions. The set of records forms a decentralized distributed ledger system that stores the records in its copies. The blockchain itself checks the authenticity of the records using a cryptographic hash function, which changes with each change in the recorded transactions. In this way, it ensures the authenticity of the stored information and eliminates the possibility of falsification or deletion of information. In practice, a transparent public database is created that is not concentrated in one place, but in many places, avoiding the possibility of a single point of failure. The most prominent representative of blockchain technology is the Bitcoin cryptocurrency [3][5][6].

Blockchain enables the creation of secure networks with high levels of cyber-protection, ideal for IoT infrastructure. IoT devices can communicate, i.e. carry out transactions and store information without the risk of it being eavesdropped, manipulated, leaked or deleted. This without the need for central certification and communication facilities. Identification and authentication can be performed by the IoT devices themselves, ensuring complete autonomy. The other serious advantage of blockchain technology is the unlimited possibility of expansion, since scalability is at the heart of the technology.

Blockchain Structure.

The blockchain structure is It consists of 2 parts - Blocks and Transactions - Fig.4 [9].

Blocks are records that are chained to each other through cryptographic hashes. Each block stores information about the corresponding transaction through a timestamp, forming a chain of records. Each block consists of a Block Header and a Block Body. Each Block Header contains the size of the block, the hash of the previous Header and its version. Information about the transaction itself is stored in the Block Body.

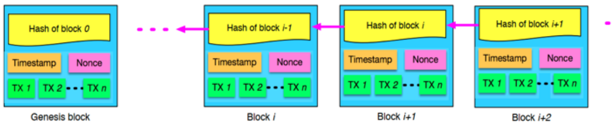

Fig. 4. Structure of blockchain

Principle of operation.

The sending party generates a transaction and sends it to all participants in the network, which are called “peers”. The legitimate recipient of the transaction certifies its identity through its digital signature, which essentially represents a public cryptographic key. The same key is unique and is used to encrypt its own transactions. Thus, the signature is a means of guaranteeing the identity of its owner. The transaction is encrypted using a cryptographic key and transmitted in the chain, with the authenticity of the transaction being guaranteed by a hash function. The hash function is the result of a mathematical calculation of the input data, and encrypted with the SHA-256 algorithm. It validates the integrity of the data in the blockchain. At the slightest change in data, the hash function changes and does not correspond to the records in the other copies of the blockchain. This ensures the impossibility of changing or deleting data. The third element is the so-called “Smart Contract”. It is an algorithm that defines the conditions to which the other participants agree. The smart contracts themselves are formed by the goals of the respective blockchain (Fig.5).

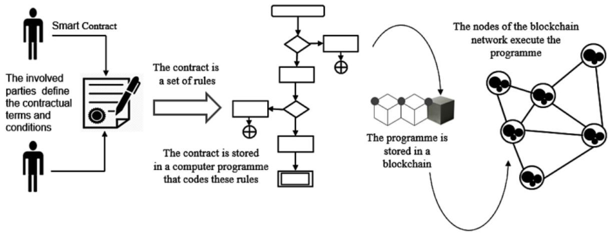
Smart Contract
The involved parties define the contractual terms and conditions
The contract is a set of rules
The contract is stored in a computer programme that codes these rules
The programme is stored in a blockchain
The nodes of the blockchain network execute the programme

Fig. 5. Concept of blockchain contract

Blockchain provides great opportunities for providing security controls related to ensuring the authenticity of a person (Access control), Data Integrity and Identity Management - Table II [11].

TABLE II. USE OF BLOCKCHAIN FOR IOT SECURITY

Security controls	Blockchain
Access Control	Use blockchain for Access Control; Decentralized access based on BC; Two factor identification based on BC.
Data Integrity	Smart contracts used for verification identity of legitimate users; Smart contracts used to manage data integrity.
Identity Management	Middleware, based on BC is used for validation of transactions; Middleware, based on BC is used for management of IoT infrastructure.

Individual security controls can be imposed on the corresponding controls in the Entities of the three-layer architecture (Fig. 3), which clearly shows the place of blockchain-related security controls that can be used to ensure a sufficient level of IoT cybersecurity (Fig.6).

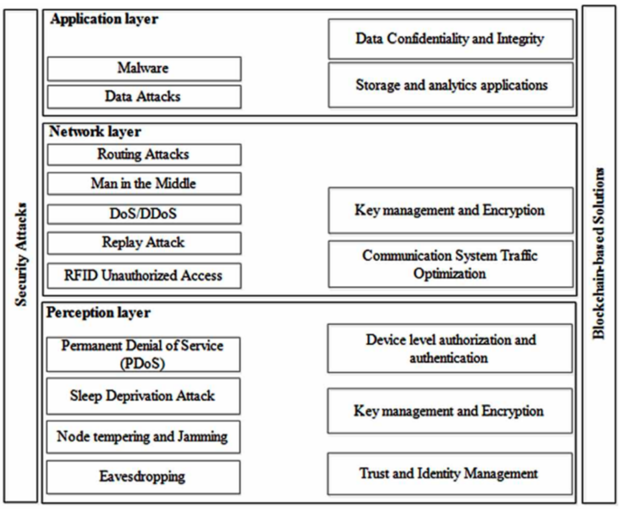
Security Attacks
Application layer
Malware
Data Attacks
Data Confidentiality and Integrity
Storage and analytics applications
Network layer
Routing Attacks
Man in the Middle
DoS/DDoS
Replay Attack
RFID Unauthorized Access
Key management and Encryption
Communication System Traffic Optimization
Perception layer
Permanent Denial of Service (PDoS)
Sleep Deprivation Attack
Node tempering and Jamming
Eavesdropping
Device level authorization and authentication
Key management and Encryption
Trust and Identity Management
Blockchain-based Solutions

Fig. 6. Blockchain-based security controls for IoT Security

Using appropriate templates, where the functionality of blockchain-related security controls is combined with classical security controls, cybersecurity systems can be designed for various IoT applications - Smart Home, Industrial IoT, IoT Automotive, Healthcare [4][12] or Education [2].

B. *Artificial Inteligence (AI)*

The recent development of machine learning (ML) and artificial intelligence (AI) provides new opportunities for the development of new and for enhancing the classic cybersecurity methods. AI significantly increases the effectiveness of cybersecurity approaches related to data analysis, such as detecting current malware, in Intrusion Detection and Prevention Systems (IDS) and (IPS) and many other security measures.

The application of AI and ML in critical applications, where a quick and adequate response is required, is especially important.

Blockchain-based artificial intelligence techniques can use decentralized learning to help ensure trust and information sharing and decision-making by many agents who can participate and collaborate in decision-making.

The convergence of blockchain and AI (Fig.7) allows training of AI models on data stored in blockchain while relying on high security and authenticity of data [13]. A very important point is that the confidentiality in this symbiosis is guaranteed by blockchain technology. On the other hand, participants (peers) in the blockchain network can rely on the capabilities of AI for the analysis of large volumes of data and, accordingly, increase the efficiency of IoT applications.

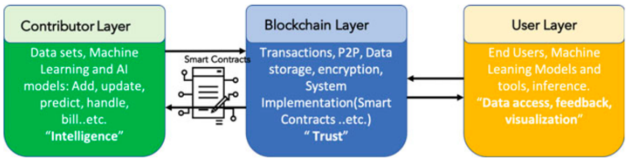
Contributor Layer
Data sets, Machine Learning and AI models: Add, update, predict, handle, bill..etc. “Intelligence”
Smart Contracts
Blockchain Layer
Transactions, P2P, Data storage, encryption, System Implementation(Smart Contracts ..etc.) “ Trust”
User Layer
End Users, Machine Leaning Models and tools, inference. “Data access, feedback, visualization”

Fig. 7. Blockchain and AI convergence model

V. DISCUSSION

It is characteristic of any new technology that when it turns from a concept into a finished product and begins to be applied on a mass scale, hidden shortcomings that were not foreseen in the theoretical part come to light.

This applies to both IoT technology and blockchain. Functionality that is theoretically an advantage quickly turns into a weak point. In both technologies, such a weak point is scalability. In practice, both technologies are infinitely expandable, but practice paints a completely different picture.

In blockchain technology, expanding the network with new nodes leads to an increase in the size of the blockchain chain itself and, accordingly, an increase in the memory requirement in which to store a copy of the blockchain. The requirements for communication bandwidth also increase due to the amount of data that is exchanged.

In IoT, we have a huge variety of hardware devices, with different parameters, communication and computing capabilities. IoT devices have different capabilities for calculating hash functions or storing the same amount of information. Accordingly, time lags appear or directly to blocking certain devices due to overload.

The use of AI in cybersecurity, in addition to its advantages, also has serious disadvantages. This is especially evident when the power of this technology is harnessed by adversaries. AI provides incredible opportunities for detecting vulnerabilities and overcoming cybersecurity measures implemented in an organization.

One of the possible solutions to the problem is the preliminary simulation of the operation of the specific IoT system and the corresponding optimization of the structure, the technologies used, communication protocols and algorithms. Other potential problems are the lack of standardization and regulatory framework to be followed by all manufacturers, leading to certain incompatibilities and difficulties. The lack of specialists in this field should not be ignored, due to the requirement for interdisciplinary knowledge and skills.

VI. Conclusion and future work

While traditional security measures can individually address device-specific, channel-specific, protocol-specific, or multi-data threats, and modern technologies such as blockchain and AI can help with this process, a systems approach is needed to fully protect the IoT infrastructure. In this approach, the IoT infrastructure and the tasks it must protect are considered holistically, specific tasks are defined, a risk analysis is performed, and appropriate technologies and security measures are selected to provide the necessary protection. In addition, solutions are selected so that the organization's resources - people, knowledge, and funds - are sufficient for its operation, maintenance, and future expansion. It is particularly important to conduct a preliminary simulation of the operation of the designed cybersecurity system for a specific IoT application, taking into account as many options as possible for the load on the devices, communication channels, and future expansion of the system. The system must be designed to be flexible not only in terms of the number of components, but also with the ability to replace key components and technologies with similar or newer ones.

ACKNOWLEDGMENT

This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. D01-74/19.05.2022.

References

[1] Internet of Things (IoT) Statistics: Market & Growth Data, By Naveen Kumar / July 5, 2025 https://www.demandsage.com/internet-of-things-statistics/?utm_source=chatgpt.com, last accessed 19.10.2025

[2] Terzieva, V., Ivanova, M., Djambazova, E., & Ilchev, S. (2025). The Role of Internet of Things and Security Aspects in STEM Education. Information, 16(7), 533. MDPI, 2025, ISSN:2078-2489 https://doi.org/10.3390/info16070533

[3] IoT Security: Advances in Authentication, First Edition. Edited by Madhusanka Liyanage, An Braeken, Pardeep Kumar, and Mika Ylianttila. © 2020 John Wiley & Sons Ltd. Published 2020 by John Wiley & Sons Ltd, ISBN: 978-1-119-52792-3

[4] Ivanova V., A. Boneva, The Internet of Medical Things Application - Challenges and Future Directions, Proceedings of the International Scientific Conference "Robotics & Mechatronics 2024", Complex Control Systems, 7, Bulgarian Academy of Sciences - Institute of Robotics, 2024, ISBN:1310-8255, ISSN:2603-4697

[5] Chawla, S.K., Sharma, N., Elngar, A.A., Chatterjee, P., & Srinivasu, P.N. (Eds.). (2024). Industrial Internet of Things Security: Protecting AI-Enabled Engineering Systems in Cloud and Edge Environments (1st ed.). CRC Press. https://doi.org/10.1201/9781003466284

[6] AlDoaies B. H., Almagwashi H., "Exploitation of the Promising Technology: Using BlockChain to Enhance the Security of IoT," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 2018, pp. 1-6, doi: 10.1109/NCG.2018.8593102

[7] Shafagh H., Hithnawi A.,Duquennoy S., Towards BlockChain-based auditable storage and sharing of IoT data. arXivpreprint arXiv:1705.08230, 2017

[8] Maleh Y.,Baddi Y., Alazab, M., Imed. (2021). Artificial Intelligence and Blockchain for Future Cybersecurity Applications, Springer Cham 2021, ISBN: 978-3-030-74574-5, DOI 10.1007/978-3-030-74575-2.

[9] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services. 14. 352. 10.1504/IJWGS.2018.095647.

[10] Ben Mnaouer, Adel, and Lamia Chaari Fourati, editors. Enabling Blockchain Technology for Secure Networking and Communications. IGI Global Scientific Publishing, 2021. https://doi.org/10.4018/978-1-7998-5839-3

[11] Dhar, S., & Bose, I. Securing IoT Devices Using Zero Trust and Blockchain. Journal of Organizational Computing and Electronic Commerce, 2020 31(1), 18–34. https://doi.org/10.1080/10919392.2020.1831870

[12] Dechev, M., Georgieva-Tsaneva, G. Overview of current technologies for data protection in healthcare, Proceedings of the International Scientific Conference "Robotics & Mechatronics 2024", Complex Control Systems, 7, Bulgarian Academy of Sciences - Institute of Robotics, 2024, ISBN:1310-8255, ISSN:2603-4697

[13] Muheidat, F., Tawalbeh, L. (2021). Artificial Intelligence and Blockchain for Cybersecurity Applications. In: Maleh, Y., Baddi, Y., Alazab, M., Tawalbeh, L., Romdhani, I. (eds) Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Studies in Big Data, vol 90. Springer, Cham. https://doi.org/10.1007/978-3-030-74575-2_1