RECENT J. (2023), 69:020-028
https://doi.org/10.31926/RECENT.2023.69.020

# Security Challenges from the Integration of AI with Blockchain

**Shih-Shuan WANG**
Transilvania University of Braşov, Romania, shih-shuan.wang@unitbv.ro
**Zsolt TOTH**
Transilvania University of Braşov, Romania, zsolt.toth@unitbv.ro
**Eugen-Silviu VRĂJITORU**
Transilvania University of Braşov, Romania, eugen.vrajitoru@unitbv.ro
**Ionela-Roxana PUIU**
Transilvania University of Braşov, Romania, ionela.puiu@unitbv.ro
**Mircea BOŞCOIANU**
Transilvania University of Braşov, Romania, boscoianu.mircea@yahoo.com

**Abstract**
The way things are done in the computer world has changed because of the Internet of Things (IoT). Therefore, it's so important to integrate cloud computing with IoT devices because of how much data such devices create and how much storage and processing power they need. The fact that users share a variety of cloud computing services among their devices in different ways makes security issues more crucial even so. In a world when unprotected data might endanger our welfare, privacy is even more important. Therefore, the IoT and cloud computing must constantly assure the users' worries about security and privacy. This study examined security concerns and potential IoT application tactics for cloud computing. According to the results, there are still significant security dangers and issues that need to be resolved. To reach that purpose, it is necessary to build the architecture and modify the present program. This article covers the many security issues that the IoT and cloud computing are experiencing, particularly the worries about user privacy and cybersecurity risks.

**Keywords**
Internet of Things, Blockchain, Security, Cloud Computing, Privacy

## 1. Introduction

The cloud and IoT are collaborating to create a framework that is heavily reliant on information repository and where security is the most crucial component in making sure that data is protected. Pay-per-use services that provide computing resources that are extremely scalable, adaptive, and storage are referred to as cloud computing [1]. A growing number of Businesses opt to shift their data from internal network infrastructure to cloud storage providers as a result of the growing popularity of cloud computing services for compute and storage (CSPs).

More apps will be developed, and those apps will have trouble connecting to cloud services because of security issues as a result of the increased demand for specific IoT devices. In the future, the ability to acquire ever-more-detailed data will allow Internet of Things technologies to provide more sophisticated services in a world teeming with intelligent objects. The emergence of several IoT devices in recent years has made it possible for users to complete their tasks quickly [1]. The use of participatory sensing is only one example, along with advanced building management systems, public monitoring, and smart city services. Due to the time-varying workloads and enormous amounts of data in IoT applications, the desired outcome will be challenging to obtain using normal processing and cloud computing.

Additionally, the third-party auditors entrusted with processing the data and preserving its integrity are still in the early stages of their development. The encryption techniques are also not yet as effective as they should be. Many government agencies are collecting more personal data about citizens each year, and as a result, it is become more difficult for the public to comprehend the implications of this data collection.

Issues with privacy are more prevalent with this type of data. Lack of awareness of these difficulties can have detrimental long-term implications, including the technology's rejection owing to issues with credibility and the failure of new technologies due to costly litigation [2]. The paper will outline the development of IoT in cloud computing, the security difficulties that arise, and the many approaches that may be used to address the problems. In order to allow secure storage and safe transit of IoT data in cloud computing. The study's main objective is to pinpoint the security concerns and procedures that IoT in cloud computing may use.

## 2. Contributions

The security issues consumers have when combining IoT devices with cloud computing are what this article tries to address. Utilized and continually improved, Internet of Things technology is being utilized to create a more live-centered, pervasive computer service that calls for massive amounts of data processing and storage.

The sector is still plagued by problems, though, and they must be resolved. It will be easier to develop solutions to the security difficulties in this article by looking at the issues from their origin. The cloud and IoT are collaborating to create a framework that is heavily reliant on data storage and where security is the most important factor in ensuring that data is protected.

In a variety of technical developments, incorporating wireless sensor networks (WSN), online personalization, Mobile applications, networks, and Radio Frequency Identification (RFID), privacy issues have been a hot study topic [3]. Despite significant contributions from these groups, the IoT is a constantly evolving concept that includes an expanding number of technologies and displays a range of shifting properties. As a result, a broad view on emerging privacy problems in the IoT is absent. IoT devices will confront significant security issues that will be challenging to solve as the technological world develops further [3]. The privacy concerns with IoT devices using cloud computing services must be taken into account and rectified in light of the potential harm that these security flaws might cause to people's lives.

## 3. Literature Review

### 3.1. Problems with Internet of Things security

IoT device hijacking or ransomware, IoT device theft, illegal internet usage, rogue devices, house invasions, and several other potential risks are some of the security concerns using IoT devices with cloud computing.

• *Malware and Ransomware*

Ransomware may infect linked wearable, audio-visual, and smart home gadgets as well as smart home appliances. Malicious program that accesses user files, encrypts them, and stops users from accessing their critical data. A ransomware attack on an IoT gadget allows the hacker to seize control of the system and demand payment from the victim in exchange for the release of their encrypted contents.

Thankfully, it still occurs infrequently. However, the hacking community and hackers themselves have a significant difficulty with this [4]. Wearable technology, healthcare trackers, and smart homes might all be at risk due to this security issue. Finding out that a person's smart home has been infiltrated and secured, or even that their smart car won't start unless a ransom is paid, is unsettling.

This might prevent the user from accessing their devices and perhaps result in the loss of their data if ransomware threats succeed, like ones that have surfaced recently. There will be some unexpected security risks brought on by the Internet of Things' quick technological development [5]. The majority of data is, however, kept on a cloud that uses strong encryption, making it extremely improbable that someone would be able to steal any valuable data. One investigation claims that certain IoT manufacturers don't provide crucial software updates and security [6].

• *There is not enough testing and there are not enough updates*

The fact that many firms making Internet of Things devices are not carefully vetted and sometimes too unorganized to effectively repair security-related software upgrades presents another security risk. Customers have significant difficulties in the event of a security breach because they frequently place their faith in producers, who are typically sure that they are in charge of product safety [7]. The Internet

of Things platform is expanding quickly, but it's also true that many manufacturing businesses are diving into the market without giving the marketing research any thought.

Shorter-term websites typically don't provide continuous updates. These upgrades are necessary due to the growing device scarcity. They therefore create the newest generation of products and invite people to begin using them without the required security precautions [8]. IoT devices may be vulnerable to multiple harmful hacker attacks and other security flaws if they are running outdated software. When an IoT gadget sends its information to the cloud, there is still another chance of downtime.

As the app is being updated, certain sections of it may cease working while other parts look for the updated bits and send the new information. It is recommended to replace the firmware as soon as possible [9] since firmware versions A49 and B06 include flaws that might make the router less secure. The right automated updates are of the utmost significance given the numerous "Internet of Things" security dangers. The maker of IoT devices has a responsibility to update, whenever a security hole or malware assault is discovered, they update their goods with the latest software.

• *Question of broadcast ip addresses to nearby hackers*

When users of IoT devices face house invasions, this is the most frightening situation for Internet of Things security issues. Right now, smart gadgets are becoming a part of every aspect of our life.

The idea of "smart houses" was created as a result of the Internet becoming accessible from many of our homes. The main issue with smart home systems is that, in the event of a security breach, there is a significant chance that they may broadcast IP addresses to nearby hackers.

In order to locate the device's user, hackers might utilize the search engine Shodan. The conclusion about misuse is that this technology may be offered to the general public and potentially find its way into criminal groups [10]. The first step in preventing that setting up each device to connect over a VPN eliminates the IoT security flaw, to consider the importance of passwords and to safeguard login information.

• *Financial crime associated with the Internet of Things*

Payment companies using the Internet of Things should be ready for a rise in identity theft and other financial crimes in the future as they roll out their Internet of Things. In the near future, the majority of these organizations will need to be able to comprehend the necessity of integrating security measures on numerous organizational levels, even while some of these companies have focused on automation and artificial intelligence.

Programs for fraud detection must constantly check their data source for fresh fraud tendencies in order to maintain greater efficacy. Due of the numerous compliance and operational problems they encounter, all financial organizations will have qualms about implementing these new models [11]. In layman's terms, there are many distinct ways that IoT security breaches might manifest themselves, IoT device hacks, smart-protocol problems, and attacks on multiple systems, among others, are included.

• *Remote access for intelligent vehicles*

A security issue like a house invasion is the hijacking of smart automobiles. Smart automobiles may become vulnerable as a result of weak Internet of Things equipment, such as when access to the vehicle is remotely hijacked [12]. The car's ability to run autonomously, such as self-driving features and other vehicle detection, may be impacted by compromised functions. Injury lawsuits involving dangers to public safety have occurred often.

A connection between losing access to the automobile and remote hacking may also exist, particularly if the hacker locks the doors and requests money before unlocking or turning on the engine. The various security breach concerns are attracting the attention of many auto and IoT device manufacturers.

But automakers like BMW and Honda are also keeping an eye on these security flaws. An entertainment system developed by Microsoft and Ford Motor is entirely accessible to these kinds of assaults [12]. A purposeful upgrading to a more secure infrastructure and software package was one of the developers' chosen options for dealing with the many kinds of these assaults. IoT devices will face a serious security concern from the upcoming release of remote-control automobiles.

• *Bad and fake IoT devices*

Being able to prevent a system from being accessed by a single device is a huge security problem. A drawback of adopting the IoT in the house is that it might get bulky if additional home appliances are

installed. Without any network authorizations, users frequently mount unauthorized and subpar IoT on protected networks. In order to collect sensitive data and information, these devices merge with the network or replace the original network units, breaching the perimeter security of the network [12, 13]. These intelligent gadgets have the ability to be modified to function as unauthorized access points, cameras, thermostats, and other kinds of equipment that are used to covertly capture network communication.

• *IoT security knowledge among users is lacking*

The peculiarities and characteristics of the Internet of Things are still being learned by many people. In terms of phishing, malware, computer viruses, and online fraud, the majority of consumers have now mastered their security difficulties. They spent some time studying about protecting their internet connection and their credit cards online before they started doing any internet banking.

However, as has been noted, IoT devices continue to have issues, not only because of the limits of both the makers and the users themselves failed to take the proper security measures to protect their networks and equipment.

Because it allows for misuse by both users and those who would be linked to their own IoT networks, a lack of computer literacy is the largest problem with the Internet of Things [13]. Hackers that utilize social engineering target people because they can most easily get around them by exploiting the Internet of Things. The 2010 attack on an Iranian nuclear facility, which was tragically awful and will always be tragic, is a significant example of the unprepared human component.

The IoT device known as a programmable logic controller was the target of the attackers, which meant that all it took for one of the employees had to insert a small flash drive into the controller, which allowed an attacker to breach the system and expose the internal network.

### 3.2. Techniques for dealing with vulnerable IoT devices

Table 1 shows the five solutions of cloud IoT cover the hazards they pose, existing defenses against such threats, and unresolved research problems. Researchers performed static or dynamic analysis on the device firmware and source code to assist them in keeping up with the most recent developments and in identifying and addressing possible vulnerabilities for additional IoT devices. Proposed an architecture to provide dynamic security analysis for the firmware of various embedded devices in 2022. These new techniques still require further work to increase their stability and precision. The architecture of a cloud-based system is subject to several network bottleneck-related limitations.

Limitations need to be resolved. In 2020, the connected devices market had a value of USD 28.24 billion, and by 2026, it is anticipated to grow to USD 94.32 billion. The network issues of the cloud-centralized computational model to more decentralized models are seen to be best solved via edge and fog computing, two major enabling paradigms. The edge layer gathers sensor data in the devices and equipment of these models, transmits it to the fog layer, which executes the treatments, and then provides the observations and results to the cloud layer through the internet.

• *Make your passwords strong and change them frequently*

It is generally accepted practice to often change or update the passwords for computers, mobile devices, and online accounts. With how advanced the Internet of Things has gotten, it ought to be commonplace by now. Making certain that the following is crucial:

- An exclusive password is given to each additional IoT device;
- Ensuring that passwords are updated many times a year, at the very least, avoiding widely used and well-known terminology;
- Using unique, incredibly challenging-to-crack codes.

The chance of someone spying on all of the passwords, or even just part of them, will grow if password managers are overused. Instead of depending on password managers, users should follow a more conventional approach and safely write down and preserve their passwords.

• *Saving the files and data locally and creating a backup*

Although cloud grid computing has many benefits, it is also a very attack-prone technology that needs to be taken extremely seriously. In exchange for the electronic device they buy, technological corporations frequently provide customers free cloud storage [14]. Despite the fact that receiving

anything for free is enticing, consumers must be cautious when it comes to security precautions:

- In order to access any files or data, cloud services require an active connection.
- While logging into the account, this cloud service can be accessed and compromised.

The users should carefully review the security measures that come with their choice of dropbox or Google accounts if they have one. In order to keep their data safe from hackers, they must also store it locally and safeguard it.

Table 1. Features of cloud IoT solutions

| **Solutions / Features** | **Amazon *AWS IoT Core*** | **Microsoft *Azure IoT Hub*** | **Google *Cloud IoT Core*** | **IBM *Watson IoT*** | **ARM *Mbed Pelion IoT*** |
|---|---|---|---|---|---|
| **Cloud Service Type** | PaaS | PaaS | PaaS | PaaS | On Premises, PaaS |
| **Hardware Support** | All devices | All devices, >1000 certified IoT hardware devices | All devices | All devices | ARM Cortex-M and Cortex-A MCU based devices |
| **Associated Storage Services** | Amazon DynamoDB, Amazon S3 | Azure CosmosDB, Azure Blob | Google Cloud Bigtable,Google Cloud Storage | IBM Cloudant, IBM Cloud Object Storage | None |
| **DedicatedOS** | Amazon FreeRTOS | Windows IoT | Android Things, Android | None | Mbed OS |
| **Language/SDK Support** | C++, Embedded C,Java, Python, JavaScript, ArduinoYun, Android, iOS | C, C#, Java, Python,Node.js | C, Java, Python, Node.js, iOS | C, C#, Mbed C++, Embedded C, Java,Python, Node.js, Node-RED | C# (.NET), Java, Python, JavaScript/Typescript |
| **Serverless Compute Services** | Amazon Lambda | Azure Functions | Google Cloud Functions | IBM Cloud Functions | None |
| **Data Protocols** | MQTT, MQTT over Websockets, HTTPS,HTTP(S) REST API(JSON) | MQTT, MQTT overWS, AMQP, AMQP over WS, HTTPS, HTTP(S) REST API(JSON) | MQTT, HTTP(S) REST API (JSON) | MQTT, MQTT over WS, HTTP(S) RESTAPI (JSON) | CoAP, OMA LwM2M, HTTP(S) REST API (JSON) |
| **Authentication** | X.509 Certificates,AWS IAM, AWS Cognito, Federated Identities | X.509 Certificates, OpenID Connect, SAS Tokens | X.509 Certificates, JSON Web Tokens(JWT) | X.509 Certificates, OpenID Connect, IBMCloud App ID (Beta) | X.509 Certificates |
| **Authorization** | AWS IoT Policy, AWSIAM Roles | OAuth 2.0, Azure Active Directory Roles | OAuth 2.0, GoogleI AM Roles | IBM Cloud IAM Roles(Beta) | Mbed Cloud Policy (ACE-OAuth) (Beta) |
| **Encryption in Transit** | TLS 1.2 | TLS 1.2 | TLS 1.2 | TLS 1.2 | TLS 1.2 (MbedTLS), DTLS |
| **Encryption at Rest** | AES-256 | AES-256 | AES256, AES128 | AES-256, AES-128,RC4-128 | No info |
| **Availability (SLA)** | ≥99.9% | ≥99.9% | ≥99.9% | ≥99.5% | No info |

• *Keeping Universal Plugs out of the way & features for playing*

When two computers are linked together, for instance, other devices can join with ease. This allows

several devices to be installed and shared within a single workgroup [15]. Evident convenience is felt by users of this platform. Due to the product's vulnerability to abuse, consumers must be cautious when using it:

- To establish connections, local networks are used by the Universal Plug & Play protocols;
- As we've already established, these networks are incredibly accessible and open to outside hacking.

• *Private networks should also be extended to IoT and smart devices*

WiFi users typically create several networks that are specifically tailored to their homes and are only accessible there. IoT and smart devices should be included in this way of building private networks to:

- Preventing the public from obtaining private data;
- Discourage the use of hostile software to commandeer IoT devices and cause mayhem;
- Encrypting the system to prevent hackers from taking control of it.

• *Making sure to periodically update the IoT device*

The Internet of Things system has to be updated by users, and the manufacturing business itself needs to allow automated updates so that the apparatus automatically looks for official upgrades. By doing this, the security of IoT devices would be ensured to be updated automatically, and hackers would be prevented from creating new ways to enter the system [16].

Occasionally, new IoT hardware offer the following benefits:

- The device's safety as it receives an upgrade with better security features to fend off assaults like Denial of Service attacks and malware (DDoS);
- Strong protection for protecting a house or business from remote invaders.

This will lead to the creation of new security procedures that will concentrate on and push fresh developments in:

- Reliable cloud IoT technology;
- Mechanisms for securing IoT systems;
- Security measures for IoT devices;
- Using artificial intelligence to identify intrusions and to identify assaults on networks for the Internet of Things;
- Robust IoT device architecture;
- IoT device security and personal data protection.

In the cloud network, IoT security is a contentious topic. Integrity breaches may occur from a variety of diverse, mutually incompatible causes.

The use of IoT technology in cloud computing is still very new [17]. The optimum solution for both customers and producers is still being sought for at this early stage of technology. One of the biggest security issues that has arisen from the IoT has been noticed:

- Malware attacks and the frequent theft of intelligent Internet of Things devices;
- Malicious IoT devices;
- Insufficient computer updates;
- Poor manufacturing quality;
- The low user competency brought on by ignorance;
- An inequitable production standard;
- Distinguishing the Internet of Things from other networks;
- Making sure passwords are distinctive and powerful;
- Staying away from Plug & Play features;
- Storing the files on backups.

## 4. Significance of the Research to the US

The United States will benefit from this research in developing the baseline cybersecurity requirements, particularly for federally owned and controlled systems.

More tactics targeted at bringing order to the IoT device security turmoil will emerge now that it is known how the vulnerabilities manifest in different devices. Many customers who had installed Amazon's Ring doorbells and cameras were quite concerned about the recent infiltration of these devices.

It will be helpful to avoid any remote access to self-driving vehicles and smart homes by understanding how to safeguard oneself. In order to safeguard consumers from cyberattacks, producers of IoT will also benefit from this research's assistance in achieving the necessary security requirements.

Additionally, it will encourage innovation since additional security measures will be built into IoT systems that use cloud services.

## 5. Conclusion

Despite growing worries about IoT device security in cloud computing, research is still being done by a number of parties to identify the problem and provide solutions. As the cloud computing sector develops, organizations will eventually see the promise of IoT.

As a result, in order to satisfy business requirements, developers will need to quadruple their cybersecurity precautions. Consumers need to understand certain security precautions to defend against some of the most frequent threats on their IoT devices. By passing laws governing IoT use, the government will play a bigger role, as it does with other technical advancements. To ensure that IoT devices are purchased with a minimal level of safety, new regulations will go into force. Currently, a number of companies sell goods that include security.

The state of wireless technology is being improved in several areas, including contact speeds and processing capacity, machine learning, convex reduction, heuristic techniques, artificial neural networks, and evolutionary algorithms. Many businesses have embraced cloud computing, which is unquestionably a useful tool. The issues with data security, however, make it uncertain whether It is dependable for safe data storage and transportation. Every business must take responsibility for keeping its data protection footprint current and implement policies that will both be able to handle any discovered defects and cope with them.

Before choosing a certain manufacturer, a user must also think about the transparency of the service, vendor lock-in, and visibility. Although these kinds of resources and technology offer immediate answers, other actions that concentrate on long-term strategy should be taken. A concern has been the lack of a security standard IoT devices have become more common, and the industry's capacity to agree on how to protect them couldn't keep up with their growing use. In order to ensure that newly identified problems are still resolved, manufacturers must ensure that users can quickly fix any concerns.

Instead of repeatedly clicking the "Ignore" button, users could upgrade their IoT programs, which is another responsibility that belongs to them. Additionally, the manufacturers must guarantee that IoT devices can update data registries.

## 6. Proposals

The authors of this study discuss how to identify threats in large streams of data. In order to lower the data dimensionality prior to the data analysis in the stream processing layer, the authors suggest a deep learning approach as a data pretreatment layer. In the proposed method, a deep learning neural network is used to automatically extract the feature from an initial feature dataset. The idea suggests greater accuracy, a smaller percentage of false-positive and false-negative results, and quicker classification times since it simplifies the original feature set.

According to the authors, any consensus process on blockchain ensures at most two out of the three qualities notwithstanding one of them since blockchain, like any distributed system, is susceptible to the CAP theorem (Consistency, Availability, and Partition Tolerance). As a result, the authors examine the blockchain network consensus proposals and note which attributes each proposal meets. The study also clarifies how probabilistic and deterministic consensus techniques vary from one another. Additionally, the authors discuss the costs and disadvantages of each consensus technique for the blockchain network.

## 7. Future Work- Blockchain and Quantum

In order to ensure security in blockchain technology, common cryptographic operations are utilized. The majority of these functions are computationally safe, making it difficult to break them without significant processing power, which is uncommon. These technologies will be impacted by the

development of quantum random number generation (QRNG), which will make it possible to decode data secured by conventional encryption techniques. A quantum random number generation (QRNG) can compromise the computational security of these functions. In contrast to conventional computers, quantum random number generations (QRNGs) may effectively process information by taking advantage of peculiar quantum features like superposition and quantum entanglement.

Unlike conventional computers, which use ordinary quantum features like superposition and quantum entanglement, quantum random number generations (QRNGs) may take advantage of uncommon quantum properties to process data quickly. As a result, it is projected that using quantum technologies in a smart environment would lead to innovations and feats of intelligence that have not yet been matched by their classical counterparts. These advancements include assured security, quick computation, and little storage usage. For the foundational elements of modern cryptography, quantum computing poses a serious danger. Within the next several decades, quantum computing is expected to become strong enough to compromise widely used security standards. Therefore, it is crucial for new gadgets and technologies to get ready for the future of quantum computing and the consequent advancement of cyberattacks. Future blockchain applications need to be prepared for quantum computing as well, as any flaw might allow for tampering with the ledger and ultimately bring the entire system to a halt. Last but not least, legacy infrastructure will be exposed without modifications to the present public key cryptography architecture to make it quantum-resistant.

The key for recently shown quantum-blockchain systems is created via quantum key distribution systems, and the authentication is based on information theory. However, such a configuration necessitates a pairwise link between each user. Utilizing quantum safe direct communication for N users with authentication or quantum digital signatures is another method for assuring quantum security. Understanding the topology of the quantum network's constraints and the proportion of unreliable (faulty) nodes on the network is crucial for these systems. One may utilize the standard family of broadcast protocols to determine the best method for developing distributed information systems that are quantum-secured after the authentication and signature processes are finished. The development of new technologies based on quantum mechanics has the potential to have a significant impact on practically every aspect of health care, including diagnosis, treatment, and data transfer. Medical data will be more secure because to the fundamentals of quantum blockchain technology, which will also stop data leaks. By adopting methods like laser microscopy, which is based on the laws of quantum mechanics, as well as s, we may also sequence DNA more quickly and address other big data issues in the field of health care. This creates the opportunity for individualized therapy based on each person's particular genetic composition.

## References


1. Veijalainen J., Kozlov D., Ali Y. (2012): *Security and privacy threats in IoT architectures*. Proceedings of 7th International Conference on Body Area Networks (BODYNETS 2012), ISBN 978-1-936968-60-2, pp. 256-262, http://dx.doi.org/10.4108/icst.bodynets.2012.250550
2. Kumar S.J., Patel D.R. (2014): *A survey on internet of things: security and privacy issues*. International Journal of Computer Applications, ISSN 0975-8887, Vol. 90, no. 11, pp. 20-26, https://research.ijcaonline.org/volume90/number11/pxc3894454.pdf
3. Inaam ul Haq M., Li Q., Hou J. (2022): *Analyzing the Research Trends of IoT Using Topic Modeling*. The Computer Journal, eISSN 1460-2067, Vol. 65, is. 10, pp. 2589-2609, https://doi.org/10.1093/comjnl/bxab091
4. Schurgot M.R., Shinberg D.A., Greenwald L.G. (2015): *Experiments with security and privacy in IoT networks*. IEEE 16th World of Wireless, Mobile and Multimedia Networks (WoWMaM), eISBN 978-1-4799-8461-9, pp. 1-6, DOI: 10.1109/WoWMoM.2015.7158207
5. Kuang B., Fu A., Susilo W., Yu S., Gao Y. (2021): *A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects*. Computers & Security, eISSN 1872-6208, Vol. 112, article 102498, https://doi.org/10.1016/j.cose.2021.102498
6. Vermesan O., Friess P. (Eds.) (2014): *Internet of Things Applications - From Research and Innovation to Market Deployment*. River Publishers, eISBN 978-87-93102-95-8, https://www.riverpublishers.com/pdf/ebook/RP_E9788793102958.pdf
7. Khoo B. (2011): *RFID as an enabler of the internet of things: issues of security and privacy*. 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing,

ISBN 978-1-4577-1976-9, pp. 709-712, DOI: 10.1109/iThings/CPSCom.2011.83
8. Lu X., Li Q., Qu Z., Hui P. (2014): *Privacy Information Security Classification Study in Internet of Things*. Proceedings of 2014 International Conference on Identification, Information and Knowledge in the Internet of Things, eISBN 978-1-4799-8003-1, pp. 162–165, DOI: 10.1109/IIKI.2014.40
9. Xiaohui X. (2013): *Study on security problems and key technologies of the internet of things*. 2013 International Conference Computational and Information Sciences, eISBN 978-0-7695-5004-6, pp. 407-410, doi: 10.1109/ICCIS.2013.114
10. Lakshmisri Surya (2015): *An exploratory study of AI and Big Data, and it's future in the United States*. International Journal of Creative Research Thoughts, ISSN 2320-2882, Vol. 3, is. 2, pp. 991-995, http://www.ijcrt.org/papers/IJCRT1133887.pdf
11. Chohan U.W. (2022): *Cryptocurrencies: A Brief Thematic Review*. http://dx.doi.org/10.2139/ssrn.3024330
12. Ziegeldorf J.H., Morchon O.G., Wehrle K. (2014): *Privacy in the internet of things: threats and challenges*. Security and Communication Networks, eISSN 1939-0122, Vol. 7, is. 12, pp. 2728-2742, https://doi.org/10.1002/sec.795
13. Christin D., Hollick M., Manulis M. (2010): *Security and privacy objectives for sensing applications in wireless community networks*. 2010 Proceedings of 19th International Conference on Computer Communications and Networks, pp. 1-6, doi: 10.1109/ICCCN.2010.5560129
14. Samani A., Ghenniwa H.H., Wahaishi A. (2015): *Privacy in Internet of Things: A Model and Protection Framework*. Procedia Computer Science, eISSN 1877-0509, Vol. 52, pp. 606-613, https://doi.org/10.1016/j.procs.2015.05.046
15. Sadeghi A.-R., Wachsmann C., Waidner M. (2015): *Security and privacy challenges in industrial Internet of Things*. 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), eISBN 978-1-4799-8052-9, pp. 1-6, DOI: 10.1145/2744769.2747942
16. Daubert J., Alexander W., Kikiras P. (2015): *A view on privacy & trust in IoT*. 2015 IEEE International Conference on Communication Workshop (ICCW), pp. 2665-2670, doi: 10.1109/ICCW.2015.7247581
17. Ishaq Azhar Mohammed (2015): *The Interaction Between Artificial Intelligence and Identity & Access Management: An Empirical study*. International Journal of Creative Research Thoughts (IJCRT), ISSN 2320-2882, Vol. 3, is. 1, pp. 668-671, http://www.ijcrt.org/papers/IJCRT1134113.pdf