Journal of Theoretical and Applied Information Technology
15th December 2021. Vol.99. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SIMPLIFIED AND SECURE AUTHENTICATION SCHEME FOR THE INTERNET OF THINGS

ZHANAT KENZHEBAYEVA[1], ZHANAR AKHMETOVA[2], RYSGUL BAINAZAROVA[3], ZHANAR KAZHENOVA[4], AIGUL SARIYEVA[5]

[1]Acting Associate Professor, Department of Computing and Software, S. Seifullin Kazakh Agrotechnical University, Republic of Kazakhstan

[2] Acting Associate Professor, Department Information Security, L.N. Gumilyov Eurasian National University, Republic of Kazakhstan

[3]Senior Lecturer, Department of Computer Science, Caspian University of Technology and Engineering named after Sh. Yessenov, Republic of Kazakhstan

[4]Doctoral Student, Department of Computing and Software, S. Seifullin Kazakh Agrotechnical University, Republic of Kazakhstan

[5]Senior Lecturer, Department of Computing and Software, S. Seifullin Kazakh Agrotechnical University, Republic of Kazakhstan

The study discusses the MQTT (Message Queuing Telemetry Transport) protocol for the Internet of Things and sensor wireless networks, its features, application options, and specific procedures. The information elements and principles of the message owner are analysed. The identification of users proposed in this study is carried out by identifying them from the Cloudant database. Such application runs on the Node.js server (JavaScript) in the IBM (International Business Machines) Bluemix environment and provides a RESTful API (Representational State Transfer Application Programming Interface) or which requires mobile client access to authenticate users. The mobile client access service is designed to activate these two APIs in any authentication application. The scientific novelty is determined by the fact that it is proposed to use separate approaches to authentication for a web application – on Cloud Directory, and for a mobile application – MobileFirst Client Access. However, both web and mobile applications use the same level of application security to allow the user to access device data. The practical significance of the study is determined by the fact that the transport layer security protocol increases the performance of the protocol and reduces computational costs, but it is not used when the initial connection to the server or in cases where the previous session has already expired. The study presents an algorithm for detecting weak symmetry breaking for analysing the randomness of a reconstructed electronic message. The study proposes a method of homomorphic encryption and authentication of users and their electronic messages in wireless sensor networks of the Internet of Things.

Keywords: *Information security, Protocol, Encryption, Interface, Programming*.

1. INTRODUCTION

IoT security is becoming a key aspect of building such wireless sensor networks [1]. Having gained access to one device, an attacker can enter the network, and then any information ceases to be confidential. This implies the relevance of information security issues in such networks, where it is necessary to take into account the limitations of the devices connected to them.

The main advantage, a distinctive feature of cloud data storage, of any deployment model, is the ability to access data from any device with Internet access [2]. Users have the ability to publish their files, share them, edit them, and view them in the browser. The cloud service also keeps a history of file changes [3]. They also have the ability to sync folders between devices – a computer, smartphone, tablet. Cloud storages allow organising shared access to a file to view or edit it by setting a certain circle of people by the user. Data retention is guaranteed by the cloud service provider's use of backup disks with file copies [4]. To protect the user's data from being

viewed by unauthorised persons, encryption of this data is used. Depending on the service, the key can be stored on the server side or on the user side. In the first case, the system ensures the confidentiality of the key and data by decrypting them for the user [5]. In the second case, the protected data can only be decrypted by the user themselves or by the person to whom the user personally transfers the key. However, if this key is lost, the user themselves will be incapable of decrypting them [6].

A comprehensive security strategy is needed to ensure an appropriate level of security for the IoT (Internet of Things) infrastructure [7; 8]. It provides data protection in the cloud, data integrity protection during transmission over the Internet, and secure communication between devices. At present, there are many cloud data stores, each of which offers a specific set of features, and has its own advantages and disadvantages. The study considers an example of DSS Cloud PCI (Data Security Standard Personal Composite Instrument) compliance analysis and discusses cloud security with consideration of possible incidents [9].

Considering the multiple security, privacy, transparency, and compliance requirements, choosing an IoT service provider becomes a very difficult task [10]. A reliable provider of IoT software and services should have extensive experience in developing such services that cover different levels of infrastructure, take into account geographical location, and provide tools for secure and transparent horizontal scaling [11]. A great advantage for the chosen supplier will also be the long-term experience in developing secure software installed on millions of computers around the world, as well as the ability to quickly and professionally assess and eliminate threats associated with the implementation of IoT.

The use of conventional methods of protecting IoT devices, such as encryption and the introduction of physical security measures, requires considerable re-engineering and adaptation, since the devices have many limitations [12]. For example, storing malicious signatures and blacklists may require a lot of disk space, which is not always possible. IoT typically consists of portable devices with low power consumption, small form factor, and limited capabilities. Often, devices operate without an operator who could enter credentials or decide how trusted a team or application is, so the devices have to make such decisions on their own. The architecture of IoT systems requires wireless networks and a cloud database for communication [13]. In previous research papers scientists discussed alternatives for methods presented in this paper. As authors thinks that MQTT is still a better solution for set applications.

2. MATHERIALS AND METHODS

The sensor network monitors environmental data using low-power electronic sensors and forms a network using a variety of XBee wireless modules. The sensor network system and proposed energy harvesting methods are configured to achieve a continuous energy source for the sensor network. The Wireless WBAN (Wireless Body Area Network) system uses medical bands to obtain physiological data from sensor nodes. Medical bands are selected to reduce interference and thus increase the coexistence of sensor node devices with other network devices available in medical centres [14].

The sensor node transmits several pulses per bit to increase the average power of the transmitted signal to improve the performance of the bit rate (BER – bit error rate). The multiple pulse per bit technique is also used as an encoding scheme to identify individual sensor nodes when more than one sensor forms a network [15]. The other gives a comprehensive overview of the latest WBAN systems, technologies, and applications [16]. By 2020, more than 50 billion devices were connected via radio. Combined with the rapid growth of the Internet of Things (IoT) market, Low-power Broadband (LPWAN – Low-power Wide-area Network) has become a popular low-speed long-distance radio technology. To meet the requirements of short range, small data transfer, low power, and low cost of the Internet of Things (IoT), the actual applications use an approach for monitoring information with a low-power broadband network based on NB-IoT (Narrow Band Internet of Things), and LoRa (Long Range). This approach uses a communication mode that contains a main node and several subnodes to adapt to the needs of large-scale information monitoring [17].

The primary purpose of protecting an IoT cloud application is to prevent unauthorised users from accessing sensitive and private data from devices [18]. Furthermore, it is necessary to prevent the software from sending unauthorised commands to the devices. The relevance of the study is conditioned by the rapid development of the architecture of users of the Internet of Things, for which this protocol is the most characteristic. To communicate with each other, the devices use various industrial protocols and one of the most popular protocols for this is MQTT. Messages in the MQTT protocol are exchanged between the client,

who may be the owner or recipient of the messages, and the broker's messages [19].

The MQTT protocol requires a mandatory data broker. This is the central idea of the technology. All devices send data only to the broker and receive data only from it. After receiving the package, the broker sends it to all devices in the network according to their subscription. For the device to receive something from the broker, one needs the latter to "subscribe" to the topic. Topics arise dynamically upon subscription or upon the arrival of a package with this topic. Topics are a convenient mechanism for organising connections of different types: one-to-many, many-to-one, and many-to-many [20]. The publisher sends the data to the MQTT broker, specifying a certain topic and subject in the message. Subscribers may receive different data from multiple publishers, depending on the subscription to the relevant topics [21]. The message consists of a header: fixed length; variable length; payload variable length fields. But MQTT have its own challenges like slower transmit cycles compared to Constrained Application Protocol (CoAP). Fast cycles are critical for systems with more than 250 devices. Resource discovery, lack of security encryption, scalability and others. So suggested implementation of this technology, especially for scalable systems is difficult at this time. Some of those problems were solved in this paper, others may be topic for future research. This article discusses the problem of user data security when using the MQTT protocol and blockchain technology. The authors described the methods presented and the types of attacks that can be applied to them.

3. . RESULTS AND DISCUSSION

The described header is of fixed length, since the main features of the MQTT protocol are implemented using the fields of this header. The first byte of the header includes four fields, three of which are special flags, and the fourth indicates the type of message. The second byte is used to indicate the remaining message length, which is the sum of the variable-length header size and the payload size. The main features of the MQTT protocol include the ability to use different service levels, which are determined by the value of this flag. This makes the MQTT protocol more flexible, unlike the CoAP-Constrained Application Protocol, whose messages can be acknowledged or processed without acknowledgment.

The publisher posts messages about the broker, and the broker posts it to the subscriber. However, the publisher does not require this message to be a guarantee to the subscriber. In other words, the subscriber may not receive this message, but the publisher does not track it. The described scenario (Figure 1) is used for cases where data loss is not critical. With constant temperature monitoring, when the loss of a single measurement does not play a significant role in the overall picture.

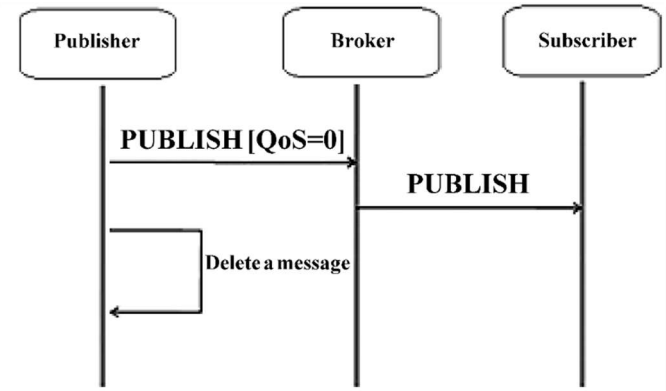

Figure 1. The "No more than one" scenario

The client publishes messages on the broker (publication). The broker saves this message and publishes it to the subscriber. Only after the message is published to the caller, the broker sends the publication confirmation to the publisher. The scenario of such interaction is presented in Figure 2. That is, until the publisher receives the subscriber's confirmation of the publication; this publication will be sent to the broker and then to the subscriber. Thus, the subscriber must receive this message at least once.

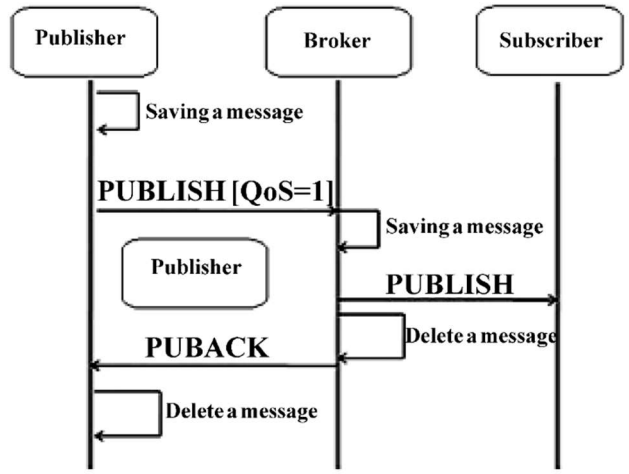

Figure 2. The "At least one" scenario

The QoS (Quality of Service) level provides the highest guarantee of message delivery

using additional confirmation and publication completion procedures. The scenario is presented in Figure 3 and is suitable for situations where you need to eliminate any loss and duplication of sensor data.

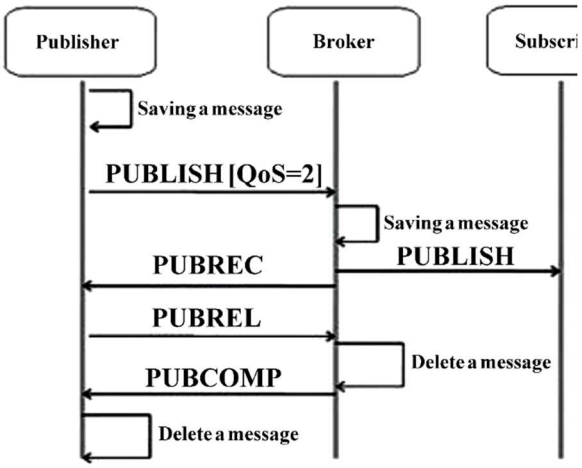

Figure 3. The "Guaranteed One" scenario

The special RETAIN parameter is used to indicate that the last message received by the broker is saved. That is, the "QoS=1" parameter in the PUBLISH message from the publisher informs the broker that messages on this topic should be saved, and when a new user joins the topic, send them this message. Establishing a connection with a connection message begins to be sent from the client to the broker (Figure 4). It specifies the following: a unique identifier for each client that connects to the broker; a flag for deleting saved messages from previous sessions for this client; a username and password for identifying and authenticating the client; a time interval regulating the transmission of ping requests and ping responses to control the disconnection of one of the parties.

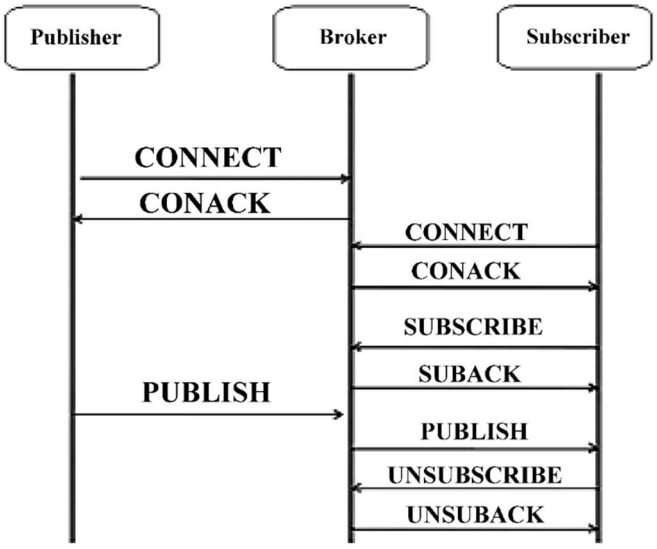

Figure 4. Established connection and messaging scenario

After the MQTT client connects to the broker, it can post a message. The publication takes place by sending a message to the broker from the client, indicating the name of the topic which the notification concerns. This field is required because the MQTT broker decides whether to send messages to the client based on which client is subscribed to; QoS, DUP (Disk Utility Program), and RITEIN; payload, where the data itself is transmitted. After receiving the PUBLISH message, the broker sends a confirmation of the publication and transmits the received message to all clients who have subscribed to this topic.

The server programme for demonstrating IoT security, which is discussed in this study, operates based on Watson IoT and transmits the received data to the Cloudant database for storage. To demonstrate IoT security, the programme encrypts some sensitive attributes of stored data during data transfer to the storage – the payload received from IoT devices. The payload arrives in JSON format and is stored in the AES (Advanced Encryption Standard) encrypted format of the Cloudant data warehouse. It is decrypted for authorised users. It is transparent to the user. The IoT data stored in the Cloudant database can be accessed directly in one of two ways: through a third-party application that provides the Cloudant API key; through developed APIs that are protected by the Bluemix security service. When the Cloudant DB service is added to Bluemix, access credentials are generated for the software, allowing it to access the Cloudant data store in a programmatic manner. The user name and password can be used to create

Cloudant API keys. Once created, the API key can be used in the same way as a normal user account.

API key and password pairs are used just like any other user account. One can pass the API key to other users to share the database with them and assign the appropriate permissions. A pair of API keys and passwords can be used in any situation where the source code has access credentials and one wants to programme the creation of multiple user accounts with different permissions. Providing direct access to the Cloudant database makes integration with third-party access unstable and expensive for technical support. In this case, an architecture is involved that uses special APIs to provide an encapsulation layer on top of the database. Special APIs hide database-related details and return device information from a specific user. Once the data is secured and transmitted using special APIs, the next step is to secure these APIs with authentication and authorisation. To call these APIs, web and mobile applications must provide the necessary authentication credentials to access the data of only the devices they have permission to access. To demonstrate the protection of specific APIs, mobile client access on the IBM Bluemix platform was used. The web application uses Cloud Directory to demonstrate SSO and IoT authorisation to support special authentication for the web application. When using this option, the sample web application must support the necessary credentials to activate the backup API.

Web applications that provide access to IoT device data must be protected with a combination of username and password for the programme users. In the sample web application, the backup user registry is used to store all user information. Furthermore, the application implements a single sign-on feature using the SSO (Single Sign-On) service, which supports three identity sources that can store user credentials: the user registry, which uses the SAML (Security Assertion Markup Language) topic exchange for authentication; the user registry, hosted in the IBM Cloud environment.

Before an application developer can integrate SSO capabilities into their programme, an administrator must create instances of the appropriate service and add identity sources. The following steps are to be performed in order to implement SSO capabilities in the sample web application. TLS False (Transport Layer Security) is based on the assumption that when the client and server already know about the connection parameters and symmetric keys, the programme data can be sent, and any necessary checks can be performed in parallel. As a result, the connection is ready to use for one iteration of messages earlier. Encryption and authentication form an integral part of every TLS connection. Next, the study considers the simplest authentication process between Alice and Bob: both Alice and Bob generate their public and private keys; Alice and Bob exchange public keys; Alice generates a message, encrypts it with her private key, and sends it to Bob; Bob uses the key received from Alice to decrypt the message and thereby verifies the authenticity of the received message.

Evidently, this scheme is built on trust between Alice and Bob. It is assumed that the exchange of public keys took place during a personal meeting, and thus Alice is sure that she received the key directly from Bob, and Bob, in turn, is sure that he received Alice's public key. Now let Alice get a message from Charlie, who she doesn't know, but who claims to be friends with Bob. To prove this, Charlie is asked to pre-sign his public key with Bob's private key, and adds this signature to Alice's message. Alice first checks Bob's signature for Charlie's keys (she knows how to do this since she already knows Bob's public key), makes sure that Charlie is indeed Bob's friend, accepts his message, and performs a known integrity check, making sure the message is from Charlie.

In the TLS protocol, these trust chains are based on certificates of authenticity provided by special bodies called certification bodies. The certification authorities carry out verification, and if the issued certificate is violated, this certificate is revoked. From the issued certificates, the already reviewed chain of trust is added. Its root is the so-called certificate signed by a major centre, the trust in which is indisputable. Most encryption data algorithms, whose robustness is based on the complexity of discrete logarithms in a finite field, are fairly easy to transfer to the case of elliptic curves. Elliptic curve cryptosystems outperform other public key systems in two important ways: the degree of protection of the computation for each key bit, and the speed of software implementation.

For a comparative analysis of the cryptosystems used for the experiment, a matrix cryptosystem was implemented based on matrix polynomials, in which the CUDA (Compute Unified Device Architecture) computing technology was used in parallel to multiply matrices and polynomials together with the modified HElib (Homomorphic Encryption library) system library.

A number of experiments were conducted with various parameters of the stability of the cryptocurrency. The study estimates the time

required to perform the following operations: encryption; decryption; multiplication (Table 1).

TABLE 1: Evaluation of the functioning of the TLS cryptosystem

Stability parameter	Encryption	Decryption	Executing a ciphertext
16	4 ms	13 ms	8 ms
24	79 ms	13 ms	15 ms
32	1.5 s	14 ms	22 ms
64	2 min	20 ms	1 s

Proceeding from the performance estimates in Table 1, it is clear that in practice, a cryptosystem based on matrix polynomials is not inferior to the improved Gentry encryption model and even benefits from the use of parallel computing technologies. An experiment was conducted on the maximum value of the parameter and at this value the authors found that the Gentry model, which is considered the fastest asymptotic, gives a model on matrix polynomials. Based on the above, it can be argued that in practice, cryptosystems designed to use homomorphic encryption must meet at least the following requirements: the set of supported mathematical functions must cover the daily needs of programmers; the accuracy and speed of calculations should not deteriorate during calculations; the stability of the algorithm should exclude a brute force attack.

Unlike light cryptography for homomorphic encryption, relevant international standards have not yet been developed, but work is underway to create acceptable solutions that can reliably process sensitive data in the cloud and for IoT brokers.

Advantages of using blockchain in IoT:

1. A decentralised structure. Similarity of approaches in IoT and blockchain. The centralised system is removed from it and the establishment of a decentralised system is ensured. This improves the probability of refusal and the performance of the overall system.
2. Safety. In blockchain, transactions are created between nodes. Therefore, the blockchain allows IoT devices to communicate with each other in a secure way.
3. Identification. In IoT, all connected devices are identified with a unique identifier. Each block in the blockchain also has a unique identifier. Blockchain is a technology that provides uniquely defined data stored in a public record.
4. Reliability. IoT nodes and the blockchain have the ability to authenticate information transmitted to the network [22]. The data is reliable because it is verified before entering the system. Only verified blockchain blocks can enter.
5. Autonomy. In the blockchain, all IoT nodes can freely communicate with any node in the network without a centralised system.

IoT allows devices to work with each other to exchange information. The blockchain-based IoT system can be divided into the following sections:

1. Physical things. The IoT provides a unique identifier that can be authenticated on the network when connected. Having a physical value at which it can exchange data with other IoT nodes.
2. Gateways are devices that work among physical things and web servers to make sure that the established connection is secure for the network.
3. The network is used to control the flow of data and find the shortest route among the IoT nodes.
4. A web server is used for storing and computing data. A blockchain is a chain of verified and cryptographic blocks of transactions conducted by a device connected to a network. Block data is stored in a digital format that is publicly transmitted and distributed. Blockchain provides secure communication in the IoT network.

Platforms with compatible use of blockchain in IoT

For the development of IoT, the following platforms are used, which are related to the blockchain technology:

– IOTA is a new platform for blockchain and IoT the so-called next generation of blockchain. This platform provides high data integrity and high transaction efficiency. The high validity of blocks provides the possibility of using fewer resources. This solves the limitations of the blockchain.
– IOTIFY. The system provides Internet-based things of the sender and the recipient. It provides a direct solution to minimise the limitations of blockchain communication as a user application technology.
– XAGE. Xage uses blockchain in its product protection, which allows it to effectively detect cyber attacks, such as compromised passwords or policies. This technology enables protection against unauthorised access when the details are stored separately in a decentralised network, and are regularly verified. If something looks wrong, it is easy to find. Xage claims that its hierarchical tree system now allows local blockchain updates to synchronise with global

updates without compromising security. In fact, for a local update, one should first form a consensus among the local nodes. It then syncs with the global blockchain, which restores local updates, changing any issues and accepting only valid changes. This hierarchical solution ensures that work can continue even when the local node is disconnected from the global network.

– SONM. It is a decentralised blockchain-based computing platform using secure web servers. IoT and blockchain are expanding business opportunities and opening up new markets where anyone or everyone can communicate in real time with authentication and security in a decentralised approach. The integration of these new technologies will change the modern world, where devices will communicate without people at different stages. The purpose of the project is to obtain secure data in the right place, in the right format, in real time. Blockchain can be used to track billions of connected Internet things, coordinate these things, enabling the processing of transactions, solving or eliminating failures, and creating a flexible ecosystem to run physical things on it. Hashing methods are used in blockchain data blocks to create confidentiality of information for users.

IoT systems with a high level of ubiquity and heterogeneity face various security and privacy threats. To guarantee the functionality of the system and achieve full user interaction, it is necessary to specify security issues and privacy concerns in the IoT. Security issues mainly include confidentiality, integrity, and authentication. Generally speaking, confidentiality ensures that the content of the data is not disclosed. Integrity ensures that data packets are not modified during transmission and prevent unauthorised users from accessing the system. Privacy concerns arise because data packets transmitted from users to IoT infrastructures may contain sensitive information. Since the information is closely related to the user's privacy, its leakage can lead to attacks on the user. Therefore, privacy measures should be provided by IoT systems. Many protection mechanisms have been proposed in various IoT scenarios. These proposed mechanisms are aimed at solving the identified security problems, since the system requirements and security models differ for different applications. Presenting these aspects will help understand the security and privacy issues in IoT systems and come up with more appropriate protection mechanisms. Therefore, security issues mainly comprise three aspects: confidentiality, integrity, and authentication. Next, the study considered the security issues and the corresponding attack methods in various IoT scenarios.

Data privacy means that the content of the data during transmission is not leaked to any user. Data content in IoT systems usually refers to the plain text content generated by the user before it performs any complex operations such as encryption and perturbations. Generally speaking, privacy is protected by encryption to protect against a possible attack. To protect the content of the data from the enemy, the attack and the ability that the attacker gains are first simulated. Let us assume that opponent A is a probable malignant user who can launch four types of attacks:

1. The attack is only for ciphertext. The lowest level of attack, which is considered the most common. In this case, the enemy only observes the communication channel and the ciphertexts in it and tries to get the main uninterrupted texts.
2. An attack with known plaintext. It concerns a scenario where an attacker can get multiple pairs of plain text or ciphertext created under a secret key.
3. An attack in a direct context. The attack is somewhat more destructive than the first two attacks, since the enemy can get ciphertexts for an unassisted selection of spatial texts.
4. Attack of the selected ciphertext. An internal attack that conditions simple texts for self-selected ciphertexts.

Integrity, that is, data integrity, which refers to the property that the contents of the data during transmission cannot be changed by any user. Generally speaking, integrity is protected by digital signatures, which is guaranteed by the impossibility of interaction in front of an attacker. Thus, an attacker can launch three types of attacks:

1. Random message attack. The attacker cannot control the signed messages, but can only observe the signatures created by the verified persons on the messages.
2. Attack of known messages. The attacker has limited control over which messages are signed, which means that the attacker must specify notifications in advance regardless of the subscriber's public key and subsequent signatures.
3. Adaptive attack of selected data. The attacker has full control over which messages are signed, which means that the attacker can select messages after they adhere to the subscriber's public key and previous signatures.

Authentication means that the recipient confirms that the received data packet is indeed from

an applicant who is related to the applicant. A typical programme is an intelligent home network, which consists of a central management system, an external user, several internal electrical appliances, and a cloud server. This type of authentication provides many convenient and interesting services, since the devices can communicate, and it allows the user to remotely control the devices when they are further away than the system. For example, a water heater can be set up before the user leaves work.

In this scientific work, the authors examined the significance of the MQTT protocol and its use in the Internet of Things. Thanks to a detailed analysis of past studies, the authors concluded that it would be advisable and effective to use the two described methods of protecting user data. Each of the methods described has its strengths and weaknesses. The use of the MQTT protocol allows to ensure the security of a specific user, but does not guarantee the security of data transmitted from the hub to the devices, while the blockchain distributes all data to all network users and allows to protect all data, but makes centralized control impossible. Attacks that can be applied to both methods are also described and analyzed in detail.

4. CONCLUSIONS

Thanks to the ubiquity of life, people are able to use more modern home services. At the same time, it concerns the importance of authentication. If the devices can be controlled by any attacker without authenticating the sender of the instructions, all the devices would turn into chaos. The Internet of Things is a concept for building distributed networks of devices, sensors, robotic systems, and machines. Evidently, critical systems require software applications and devices to develop a solution to the situation regardless of the quality of the Internet connection, as well as in the event of a complete shutdown. This study covers topics such as secure storage of Internet of Things data, the transfer of this data through a secure interface of mobile devices and web applications. All the key tools provided by the MQTT protocol for information security are also considered.

To improve the security of messages, it is proposed to use a transport layer security protocol that uses various cryptographic methods. The authors of this study propose a homomorphic encryption of these protocols. The infrastructure of secure authentication in the Internet of Things is being investigated.

The minimal overhead, the availability of service classes and the hierarchical structure of topics are the indisputable advantages of the MQTT protocol, as evidenced by the wide variety of both client and server software, including open-source software. Therefore, a paradigm shift from transport-level routing to application-level routing can be observed. Further research will focus on the encryption of chaotic electronic messages based on dynamic mathematical models and chaotic algorithms of data transmission protocols.

REFERENCES

[1] X. Zhang and F. Wen, "A novel anonymous user WSN authentication for Internet of Things," *Soft Computing*, vol. 23, no. 14, 2019; pp. 5683-5691.

[2] F. Asadpour and S. Ghanbari, "Presenting a new method of authentication for the internet of things based on RFID," *Advances in Intelligent Systems and Computing*, vol. 700, 2018; pp. 506-516.

[3] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Security and Communication Networks*, vol. 2017, 2017; article number 6562953.

[4] J. Liu, Y. Xiao and C. L. P. Chen, Authentication and access control in the Internet of things. In: *Proceedings – 32nd IEEE International Conference on Distributed Computing Systems Workshops, ICDCSW*. Piscataway: IEEE, 2012; pp. 588-592.

[5] Zh.E. Kenzhebaeva, G.Zh. Isabaeva, and Zh.K. Zhunusova, "Cyber security," *Reports of NAS RK*, vol. 6, no. 322, 2018; pp. 21-24.

[6] B. Yu and H. Li, "Anonymous authentication key agreement scheme with pairing-based cryptography for home-based multi-sensor Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019; pp 1-11.

[7] C. Zhou, Y. Yang and Y. Wang, "The two-way trusted authentication mechanism of the internet of things for the community pension," *Lecture Notes in Electrical Engineering*, vol. 463, 2019; pp. 2439-2447.

[8] Zh.E. Kenzhebaeva, Cybersecurity and its ambiguous status Digitalization of the economy and society: problems, prospects, security. In: *Proceedings of the international scientific and practical conference Digitalization of Economy and Society: Problems, Prospects, Security*. Donetsk: "Digital Printing House", 2019; pp. 688-702.

[9] H.-L. Wu, C.-C. Chang and L.-S. Chen, "Secure and anonymous authentication scheme for the Internet of Things with pairing," *Pervasive and*

Mobile Computing, vol. 67, 2020; article number 101177.

[10] T. Yang, G.-H. Zhang, L. Liu and Y.-Q. Zhang, 2020. A survey on authentication protocols for internet of things. *Journal of Cryptologic Research*, vol. 7, no. 1, 2020; pp. 87-101.

[11] Z.-Z. Liu, H.-Y. Shu, and S.-Y. Dong, "Application of group-authentication in internet of things with the trend of network integration," *Nanjing Li Gong Daxue Xuebao/Journal of Nanjing University of Science and Technology*, vol. 36, no. Sup.1, 2012; pp. 206-211.

[12] A. Wang, Z. Li, and X. Yang, "An efficient message-attached password authentication protocol and its applications in the internet of things," *Communications in Computer and Information Science,* vol. 214, no. 1, 2011; pp. 263-269.

[13] B. Zhao, P. Liu, X. Wang and I. You, "Toward efficient authentication for space-air-ground integrated Internet of things," *International Journal of Distributed Sensor Networks*, pp. 15, no. 7, 2019; pp 1-14.

[14] U. M. Qureshi, G. P. Hancke, T. Gebremichael, U. Jennehag, S. Forsström, and M. Gidlund, Survey of proximity-based authentication mechanisms for the industrial internet of things. In: *Proceedings IECON 2018 – 44th Annual Conference of the IEEE Industrial Electronics Society*. Piscataway: IEEE, 2018; pp. 5246-5251.

[15] B. Yu, C. Yang, and J. Ma, Continuous authentication for the internet of things using channel state information. In: *IEEE Global Communications Conference, GLOBECOM – Proceedings*. Piscataway: IEEE. 2019; pp 1-6.

[16] F. Chu, R. Zhang, R. Ni and W. Dai, An improved identity authentication scheme for internet of things in heterogeneous networking environments. In: *Proceedings – 16th International Conference on Network-Based Information Systems, NBiS,* Piscataway: IEEE, 2013; pp. 589-593.

[17] T. Limbasiya and A. Karati, Cryptanalysis and improvement of a mutual user authentication scheme for the Internet of Things. *International Conference on Information Networking,* 2018; pp. 168-173.

[18] L. Liu, B. Fang, and B. Yi, A general framework of nonleakage-based authentication using CSP for the internet of things. In: *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*). Cham: Springer, vol. 8710, 2014; pp. 312-324.

[19] J. Xingzhong, X. Qingshui, M. Haifeng, C. Jiageng, and Z. Haozhi, The Research on Identity Authentication Scheme of Internet of Things Equipment in 5G Network Environment. In: *International Conference on Communication Technology Proceedings, ICCT*. Piscataway: IEEE, 2019; pp. 312-316.

[20] Y. Chung, S. Choi, and D. Won, "Anonymous Authentication Scheme for Intercommunication in the Internet of Things Environments," *International Journal of Distributed Sensor Networks*, vol 11, no. 11, 2015; pp. 1-13.

[21] Y.-P. Kim, S. Yoo and C. Yoo, DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In: *IEEE International Conference on Consumer Electronics, ICCE*. Piscataway: IEEE, 2015; pp. 196-197.

[22] B. Flores, and T. Tran, T, "Use of Neural Networks in the Formation of a High-Quality Smoothed Audio Signal," *Scientific Herald of Uzhhorod University. Series "Physics"*, vol. 49; 2021; pp. 35-42.