International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 1, February 2024, pp. 479~487
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i1.pp479-487

Enhancing cryptographic protection, authentication, and authorization in cellular networks: a comprehensive research study

Khuralay Moldamurat, Yerzhan Seitkulov, Sabyrzhan Atanov, Makhabbat Bakyt, Banu Yergaliyeva
Department of Information Security, Faculty of Information Technology, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan

Article Info

Article history:

Received Jul 16, 2023
Revised Sep 10, 2023
Accepted Sep 12, 2023

Keywords:

Authentication methods
Authorization methods
Blockchain-based authentication
Cellular networks
Cryptographic protection
Data encryption
Information security

ABSTRACT

This research article provides an extensive analysis of novel methods of cryptographic protection as well as advancements in authentication and authorization techniques within cellular networks. The aim is to explore recent literature and identify effective authentication and authorization methods, including high-speed data encryption. The significance of this study lies in the growing need for enhanced data security in scientific research. Therefore, the focus is on identifying suitable authentication and authorization schemes, including blockchain-based approaches for distributed mobile cloud computing. The research methodology includes observation, comparison, and abstraction, allowing for a comprehensive examination of advanced encryption schemes and algorithms. Topics covered in this article include multi-factor authentication, continuous authentication, identity-based cryptography for vehicle-to-vehicle (V2V) communication, secure blockchain-based authentication for fog computing, internet of things (IoT) device mutual authentication, authentication for wireless sensor networks based on blockchain, new secure authentication schemes for standard wireless telecommunications networks, and the security aspects of 4G and 5G cellular networks. Additionally, in the paper a differentiated authentication mechanism for heterogeneous 6G networks blockchain-based is discussed. The findings presented in this article hold practical value for organizations involved in scientific research and information security, particularly in encryption and protection of sensitive data.

Corresponding Author:

Yerzhan Seitkulov
Department of Information Security, Faculty of Information Technology, L.N. Gumilyov Eurasian National University
Satpayev str., Astana, Kazakhstan
Email: yerzhan.seitkulov@gmail.com

1. INTRODUCTION

The rapid proliferation of smart devices and their widespread connectivity has had a profound impact on the delivery of mobile services worldwide. In this interconnected environment, ensuring the security of transmitted data primarily depends on the process of authentication. Authentication serves as a fundamental defense mechanism against unauthorized access to sensitive applications or devices, both offline and online as shown in Figure 1. Traditionally, transactions were authenticated through physical means, such as the use of wax seals [1]–[10].

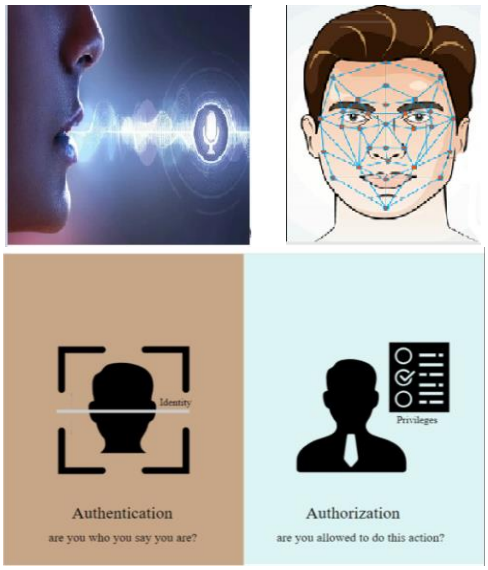


Figure 1. Conceptual examples of authentication

Figure 1 illustrates two conceptual examples of authentication. The left side represents a traditional physical method, symbolized by a wax seal stamp, to physically verify the authenticity and integrity of a transaction or document. On the right side, a digital authentication method is depicted, represented by a lock symbol and a fingerprint, symbolizing the use of digital technologies like biometric authentication or encryption keys to validate and secure access to digital systems or data [11], [12].

Sharing passwords can immediately jeopardize an account, and a variety of attacks, such as dictionary attacks, rainbow tables, or social engineering techniques, can be attempted by unauthorized users. Therefore, when employing this type of authentication, it is crucial to consider minimum password complexity requirements [13]. Recognizing the limitations of single-factor authentication (SFA), obviously that two-factor authentication (2FA) emerged as a logical progression. 2FA links representative data, such as username and password, with a personal possession factor like a smart card or phone [14].

Subsequently, multi-factor authentication (MFA) was to provide a quite high level of information security and enable permanent protection of computing devices (servers) and critical services against unauthorized access. MFA entails the use of more than two categories of credentials, often incorporating biometrics that automatically identify individuals on their biological and other behavioral features. This advancement in authentication methods bolsters security by requiring users to provide confirmation of their identity based on two and/or more different factors [5], [11], [14]. Figure 2 illustrates the development of authentication methods.

Figure 2 showcases the progression of authentication methods over time, starting with SFA and evolving to 2FA, culminating in MFA utilizing biometric factors. Arrows depict the transition from one authentication method to another. In recent times, there has been notable progress in online applications as organizations strive to meet the evolving demands of customers. Online identity access management (IAM) plays a vital role in securely authenticating customers during daily financial transactions. Surveys have highlighted several types of client authentication protocols implemented for secure data transfer, which include SFA and MFA. These protocols employ diverse authentication factors, evaluated based on parameters such as i) collectability, ii) universality, iii) uniqueness, iv) usability, and v) performance. To enhance security and avoid the use of sensitive biometric information, a framework has been proposed to identify important missing factors and enable efficient authentication using built-in sensors, like those found in vehicles [6], [12], [15].

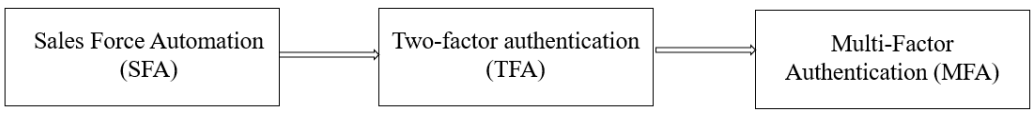


Figure 2. Evolution of authentication methods

Current biometric approaches, such as face recognition and fingerprint recognition utilized in smart devices, aim to enhance usability compared to traditional authentication methods. However, the drawback of physiological biometrics lies in the static nature of these characteristics, rendering them susceptible to replication by adversaries [7], [11], [16]. Authentication of user can occur on the device as well as on server-side. Authentication of device-side occurs fully on the self-device, while service/cloud-side authentication requires users to provide authentication credentials to their server, which in turn verifies the user's identity and grants access to the service upon successful authentication. The availability of high-performance computing and servers' resources and on-demand cloud services enables users and organizations to use cloud-based data processing, storage, and easy access to various services, including convenient data backup [17].

However, this article examines a potential concern with session-oriented approaches. The issue arises when a user leaves their computer or device unattended, allowing malicious users to gain unauthorized access to the device or any other services in which the user is logged into. This problem can be significantly mitigated by implementing standard security mechanisms that continually re-authenticate authenticate the user during a session. Authentication of the user methods can be categorized as active or passive. Active authentication requires constant attention user attention or other action, such as PIN-code, entering a password, as well as utilizing a fingerprint scanner. On the other hand, we understand that passive authentication is a transparent and seamless type of authentication that operates in the background but without user notification or attention [9], [13], [18]. To effectively address information threats, it is crucial to ensure reliable data encryption, alongside the implementation of an efficient system to detect and prevent such threats. This article will explore the concept of robust data encryption and its significance in maintaining strong information security.

2. RESEARCH METHOD

To address these issues, the following research questions were investigated in this study. As cellular vehicle-to-everything (C-V2X) technology gains popularity and widespread usage, vehicles are becoming mobile devices facing various network security challenges. The integration of communication, transportation, and automotive technologies in C-V2X exposes vulnerabilities such as forgery or eavesdropping, as well as spoofing and denial of service attacks (DoS attack). Addressing all these security challenges requires the widespread adoption and scale commercial application of technology of C-V2X. Therefore, the development of C-V2X security technology needs to be synchronized with its communication technology [10], [14], [19].

Previous schemes and systems internet of things (IoT) and fog environments prioritize authentication and use blockchain technology to enhance information security and also for decentralization. However, many of these schemes and systems rely on the Ethereum blockchain, while others depend on centralized databases, causing certain limitations. This article proposes a decentralized authentication system of fog and IoT, which based on technology of Neo blockchain as an improvement over existing systems, aiming to overcome the limitations associated with Ethereum-based decentralized authentication systems. Table 1 provides a concise overview of common cyberattack scenarios in an IoT system.

Cyberattack scenarios can target the original encryption key and the session key used for authentication and data transfer [20]–[25]. A Merkle tree structure organizes data by hashing transactions and recursively generating hash values until a final Merkle root digest, representing all transactions, is obtained. The Merkle root is added to the block header, creating a block hash that serves as the block's identifier. In this study, node information and network data were stored in blocks, with each block accommodating 100 data units. New blocks are created once sufficient data is collected.

Table 1. Description of cyberattack scenarios

ID	Attack scenario: definition
I	Replay Attack: Maliciously replaying or delaying legitimate traffic in order to disrupt communications.
II	Machine learning (ML) attack: This is using ML algorithms to predict response of physical unclonable function (PUF) by using PUF Challenge-Response Pair (CRP).
III	"Man in the Middle" Attack: Covertly intercepting and possibly altering transmitted information between two parties.
IV	Invasive attack: Physically accessing a hardware semiconductor, such as an Integrated Circuits, to extract secrets or understand its structure.
V	Firmware attack: Remotely modifying or injecting malicious software into an IoT device in order to compromise the secret key which stored.
VI	Listening attack: covertly searching for confidential data in communication networks with insecure canal net.
VII	Spoofing/Spoofing Attacks: Masquerading as a trusted node within an IoT system
VIII	"Side channel" attack: Exploiting physical access to the PUF, with potential types including invasive, semi-invasive and non-invasive attacks. These attacks analyze factors like power consumption to recover the PUF's secret key. They can be active or passive depending on the attacker's manipulation or data collection approach.

3. RESULTS AND DISCUSSION

In this section, the results of the research are explained and comprehensively discussed. Results are presented in figures, graphs, tables and other forms that the reader may easily understand. In this study, an examination of various authentication and authorization methods in cellular communication networks was conducted. One of the proposed approaches is a simplified PUF that is based scheme of mutual authentication for wireless telecommunication networks, which ensures provable security. The scheme consists of several steps, including i) registration by user, ii) registration of sensor node, iii) key agreement, iv) mutual authentication, and v) password change. During the key agreement and mutual authentication phase, the worker initiates a message of authentication to the gateway, establishing a session key between the worker, sensor node, and gateway. This enables the worker to receive patient information from the sensor node.

With the worldwide transition from 4G to 5G mobile networks, leveraging advancements in wireless and networking technologies, significant improvements are expected. 5G offers quite data transfer rates, increased bandwidth, and low latency, enabling a large number of IoT devices to be connected. The selection of authentication and privacy schemes for 4G and 5G networks was based on a literature search using relevant keywords and assessment criteria. These schemes aim to address the unique security challenges found within 5G networks.

The proposed blockchain-based differentiated authentication mechanism (BDAM) enhances authentication processes in heterogeneous 6G networks. It builds upon the differentiated authentication framework based on blockchain. The mechanism utilizes blockchain technology to differentiate authentication methods. Figure 3 provides a simplified illustration of the mechanism, excluding the encryption and also illustration decryption of messages between user equipment (UE) and authentication authority (AA) for clarity.

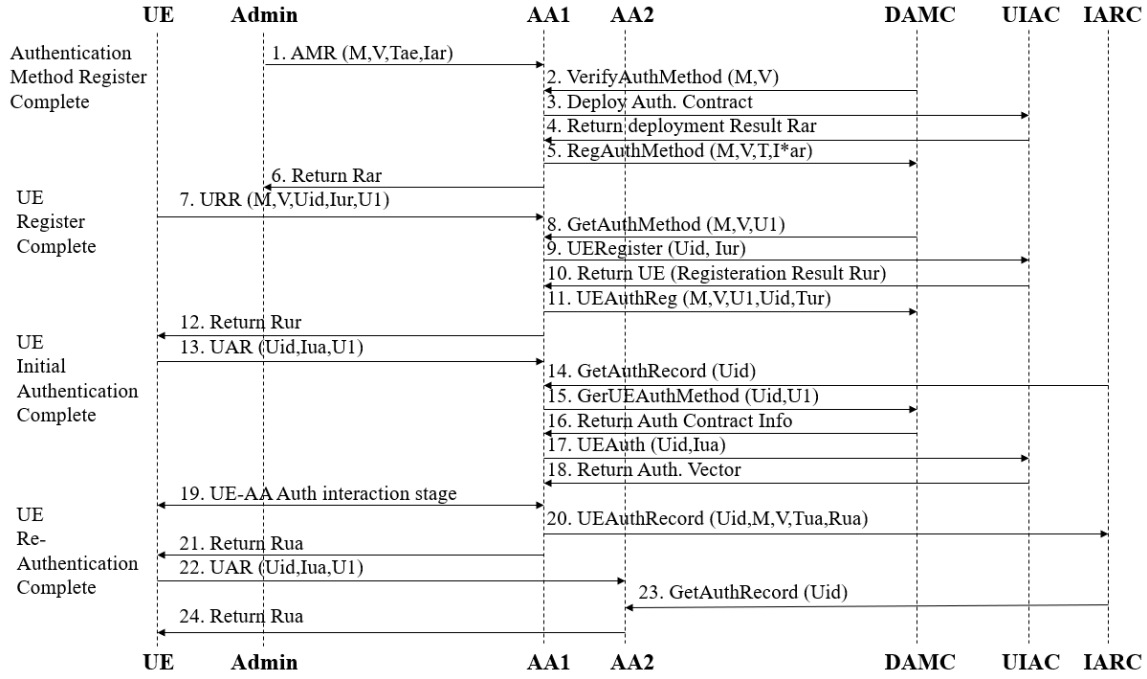


Figure 3. Blockchain based authentication mechanism

In the blockchain-based differentiated authentication mechanism, various user identity authentication components (UIACs) represent different authentication methods. The distributed authentication method controller (DAMC) is deployed within the authentication control system (ACS) to manage these UIACs in a unified manner. During the registration of the authentication method, the network access communicates securely with the authentication agent through a dedicated management interface. Furthermore, the proposed Authentication and authorization scheme which based on blockchain for distributed mobile cloud computing presents a system model, as depicted in Figure 4. The figure illustrates the involvement in the scheme two types of participants and the blockchain network.

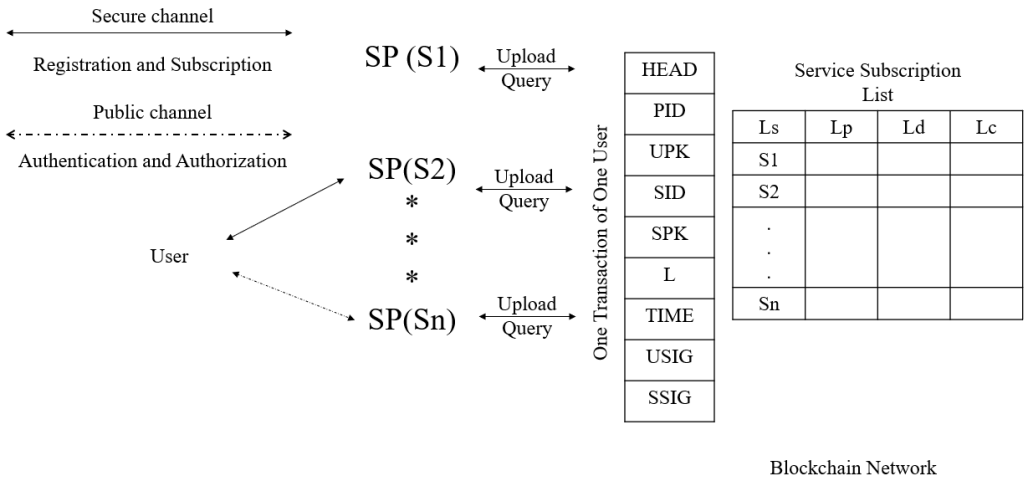


Figure 4. System architecture and transaction structure: recording user's subscription to *n* service providers (SPs)

The authentication and authorization phase in our system involves the interaction between mobile users (Ui) and service providers (Sj). After registering on a randomly selected service provider, mobile users can access hierarchical cloud services provided by the service providers. Service providers, acting as semi-trusted entities, verify the identity, privileges, and service duration of the mobile users before granting them access to the hierarchical cloud services.

During this stage, mutual authentication occurs between the user of mobile (Ui) and the service provider (Sj). Additionally, the service provider consults the service subscription list (L) to determine the appropriate service level (LevSj) that the user can access during the service's duration (DaySj) [21], [25]. Remix Solidity is a widely used development environment for smart contract development, known for its user-friendly interface and simplicity [11], [25]. The smart contract also includes functions that display transaction options for different levels of identification. Figure 5 illustrates a code snippet representing a function that presents transaction types with varying levels of protection.

To initiate the local test blockchain, the ganache command-line interface (Ganache-CLI) tool is utilized. It generates ten test accounts on the local test blockchain. Launching the Ganache-CLI tool from the bash console allows for an intermediate check of the smart contract's functionality. The tool is invoked by executing the command "ganache-cli" in the “node.js” console, which then displays the ten test accounts. The test network can be accessed at localhost:8545.

Once the test blockchain network is established, the smart contract is compiled in the Remix integrated development environment, using the ".sol" extension. In the "Run" tab of the development environment, the "Environment" field is configured to utilize the web3 provider address created with ganache-cli, which is http://localhost:8545. The available test accounts are displayed in the "Account" field of the development environment, as illustrated in Figure 6.

```
function getOption1 (string pollName) public view returns (string) {
    require(doesPollExist(pollName));

    return polls[pollName].option1;
}

function getOption2 (string pollName) public view returns (string) {
    require(doesPollExist(pollName));

    return polls[pollName].option2;
}

function getOption3 (string pollName) public view returns (string) {
    require(doesPollExist(pollName));

    return polls[pollName].option3;
}
```

Figure 5. Transaction type display function with varied levels of protection

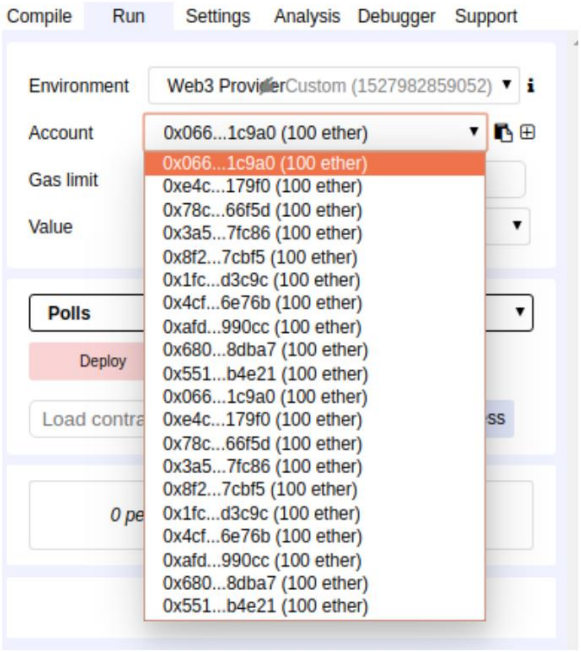


Figure 6. Connecting remix to the ganache-CLI testnet

Following the aforementioned steps, the subsequent task is to deploy the smart contract by clicking on the "Deploy" button in the Remix integrated development environment and test its functionality. During this process, relevant information about the survey being created is provided in the constructor. The four authentication methods mentioned above align with the depicted authentication process in Figure 7.

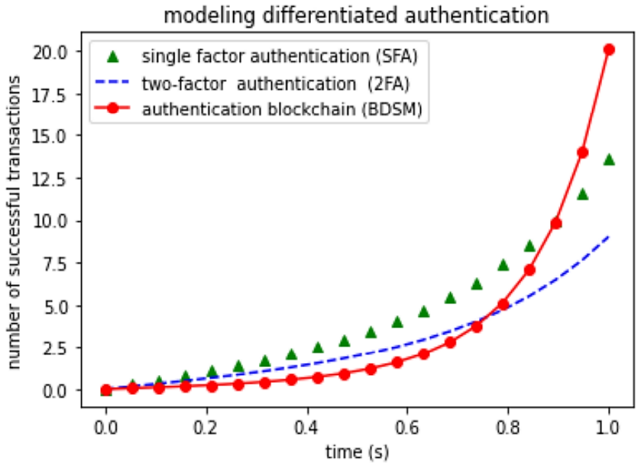


Figure 7. The number of authenticated transactions in BDAM and without BDAM in the range of 0–100 s

Figure 7 demonstrates that each authentication device (AD) can only respond to user authentication requests (UARs) if the corresponding authentication methods are deployed. In the case of 2FA, it utilizes image-based authentication, where the user's key facial points are scanned and recognized. However, this method is resource-intensive and heavily reliant on factors such as image quality and lighting. Processing time is not significant when dealing with individual images, but it becomes a challenge when working with videos due to processing delays. The complexity of authentication increases exponentially with the number of simultaneous transactions. Despite its advantages, this method remains susceptible to several attacks such as eavesdropping, “man in the middle” attacks, replay, service denial and denial attacks.

On the other hand, full-spectrum authentication (FSA) is a widely used authentication method with high processing speed and stability. It exhibits consistent performance with a nearly linear dependence even with more than ten simultaneous transactions. However, this method is vulnerable to common types of attacks, including eavesdropping, man-in-the-middle attacks, DoS attacks, replay, denial attacks, and others.

In contrast, the blockchain-based differentiated authentication mechanism overcomes these vulnerabilities. However, as the number of concurrent transactions exceeds 15, processing time undergoes an exponential increase. This is primarily due to the significant growth in user logs and the necessity to update all entries in real-time. Based on this assessment, it can be concluded that BDAM allows for flexible and dynamic deployment of authentication methods, facilitating unified management while also offering high scalability. However, this method requires algorithm and hardware modifications to accelerate record processing.

4. CONCLUSION

This article delves into the exploration of novel methods of cryptographic protection and advancements in authentication and authorization techniques in cellular communication networks, with a specific focus on high-speed data encryption. To comprehensively address the research topic and tackle the underlying problem, a thorough review of various solutions has been conducted. This includes an analysis of MFA approaches, challenges, requirements and attacks, as well as improved performance methods for fog computing and mutual authentication of IoT devices using physical non-cloneable functions and hashing.

The importance of digital security cannot be overstated, and MFA plays a crucial role in safeguarding sensitive data. By employing multiple authentication methods, we introduce an additional layer of protection, and that is making it significantly more challenging for unauthorized users to gain access. Understanding the significance of MFA and the various authentication factors is essential for making informed decisions when securing digital assets. “Open Authentication”-compliant solutions have become the industry standard for MFA, and organizations should consider implementing such solutions to ensure secure authentication.

Blockchain-based methods for distributed mobile cloud computing have been identified as particularly suitable for authentication and authorization schemes. This work includes the programmatic modeling of an authentication protocol or wireless sensor networks based on blockchain and the testing of an authentication and authorization scheme for hierarchical cellular network services based on blockchain. The proposed scheme enables "single user" sign-on without the need for a trusted other party, reducing the associated overhead of establishing a secure cell session. It also allows for the loading of all relationships of authorization between a user of mobile and other users, including devices of IoT, with just one transaction, providing flexibility and avoiding multiple updates. Additionally, it prevents the reusing expired privileges in previous transactions, mitigating double spending attacks. Transactions are stored in plaintext as a transparent blockchain, and user's registration information is publicly accessible. Therefore, the scheme which is proposed is designed for permissioned blockchains and cannot be applied directly to private blockchains. Future work will focus on modeling and hardware implementation on field programmable gate array (FPGA) for decentralized authorization while maintaining access privileges in ciphertext, which will significantly enhance transaction speed. The research presented in this article contributes to addressing the challenges of enhancing information security in data transmission, particularly in cellular communication networks.

ACKNOWLEDGEMENTS

This research is funded by the SC of the MSHE of RK (Program No. BR18574045).

REFERENCES

[1] B. Patil and S. R. Biradar, “An efficient authentication and key-distribution protocol for wireless multimedia sensor network,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 27, no. 1, pp. 347–354, Jul. 2022, doi: 10.11591/ijeecs.v27.i1.pp347-354.

[2] M. S. Mispan, A. Z. Jidin, M. R. Kamaruddin, and H. M. Nasir, “Proof of concept for lightweight PUF-based authentication protocol using NodeMCU ESP8266,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 24, no. 3, pp. 1392–1398, Dec. 2021, doi: 10.11591/ijeecs.v24.i3.pp1392-1398.

[3] A. K. Raghunath, D. Bharadwaj, M. Prabhuram, and A. D, “Designing a secured audio based key generator for cryptographic symmetric key algorithms,” *Computer Science and Information Technologies*, vol. 2, no. 2, pp. 87–94, Jul. 2021, doi: 10.11591/csit.v2i2.p87-94.

[4] M. Zostant and R. Chataut, “Privacy in computer ethics: Navigating the digital age,” *Computer Science and Information*

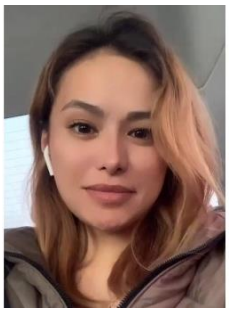
Technologies, vol. 4, no. 2, pp. 183–190, Jul. 2023, doi: 10.11591/csit.v4i2.p183-190.
[5] M. N. A. A. Afif, "Design and implementation maximum power point tracker (MPPT) flyback converter using fuzzy logic ccontroller," *Intellectual Journal of Energy Harvesting and Storage*, vol. 1, no. 1, May 2023, Accessed: Sep. 26, 2023. [Online]. Available: https://iaesprime.com/index.php/ehs/article/view/176
[6] R. Shekhar and D. Mala, "A review on design and analysis of piezoelectric energy harvesting systems," *Intellectual Journal of Energy Harvesting and Storage*, vol. 1, no. 1, May 2023, Accessed: Sep. 26, 2023. [Online]. Available: https://iaesprime.com/index.php/ehs/article/view/309
[7] V. Goel, M. Aggarwal, A. K. Gupta, and N. Kumar, "blockchain-based Aadhar system: distributed authentication system," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 20, no. 6, pp. 1239–1247, Dec. 2022, doi: 10.12928/TELKOMNIKA.v20i6.24231.
[8] A. M. Al-Ghaili, H. Kasim, M. Othman, and W. Hashim, "QR code based authentication method for IoT applications using three security layers," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 4, pp. 2004–2011, Aug. 2020, doi: 10.12928/TELKOMNIKA.V18I4.14748.
[9] A. A. Majeed, B. A. Mahmood, and A. C. Shakir, "A secure and energy saving protocol for wireless sensor networks," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 10, no. 6, pp. 3353–3360, Dec. 2021, doi: 10.11591/eei.v10i6.2796.
[10] A. A. M. Lehmoud, N. T. Obeis, and A. F. Mutar, "Design security architecture for unmanned aerial vehicles by 5G cloud network based implementation of SDN with NFV and AI," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 1, pp. 403–410, Feb. 2023, doi: 10.11591/eei.v12i1.4239.
[11] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing and Management*, vol. 58, no. 2, p. 102468, Mar. 2021, doi: 10.1016/j.ipm.2020.102468.
[12] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7669–7678, Nov. 2021, doi: 10.1109/TII.2021.3049141.
[13] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, Mar. 2021, doi: 10.1109/TDSC.2019.2904274.
[14] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in iot-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021, doi: 10.1109/JIOT.2020.3030308.
[15] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1338–1351, 2022, doi: 10.1109/TDSC.2020.3022797.
[16] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022, doi: 10.1109/JIOT.2021.3113321.
[17] X. Wang and J. Yang, "A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient," *Information Sciences*, vol. 569, pp. 217–240, Aug. 2021, doi: 10.1016/j.ins.2021.04.013.
[18] M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 65–84, Jan. 2021, doi: 10.1109/JIOT.2020.3020076.
[19] M. Azrour, J. Mabrouki, A. Guezzaz, and Y. Farhaoui, "New enhanced authentication protocol for internet of things," *Big Data Mining and Analytics*, vol. 4, no. 1, pp. 1–9, Mar. 2021, doi: 10.26599/BDMA.2020.9020010.
[20] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 507–523, Jan. 2022, doi: 10.1109/TDSC.2020.2974220.
[21] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, pp. 1–31, Jan. 2018, doi: 10.3390/cryptography2010001.
[22] Denis Starkov, "API authentication and authorization requirements," *GitHub*. https://starkovden.github.io/authentication-and-authorization.html (accessed Aug. 04, 2023).
[23] A. H. Y. Mohammed, R. A. Dziyauddin, and L. A. Latiff, "Current multi-factor of authentication: Approaches, requirements, attacks and challenges," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, pp. 166–178, 2023, doi: 10.14569/IJACSA.2023.0140119.
[24] A. F. Baig and S. Eskeland, "Security, privacy, and usability in continuous authentication: A survey," *Sensors*, vol. 21, no. 17, Art. no. 5967, Sep. 2021, doi: 10.3390/s21175967.
[25] Q. Li, "A V2V identity authentication and key agreement scheme based on identity-based cryptograph," *Future Internet*, vol. 15, no. 1, Art. no. 25, Jan. 2023, doi: 10.3390/fi15010025.

BIOGRAPHIES OF AUTHORS

Khuralay Moldamurat was educated at the I. Zhansugurova Zhetysu State University, specialist physics and informatics. Academy of Economics and Law named after academician U.A. Dzholdasbekov, bachelor of specialty finance, Turkish State University, Ankara, 2008, 2010 candidate of technical sciences (approved by the Higher Attestation Commission RK dated June 30, 2011, protocol No. 6. Diploma No. 0006248) at the dissertation council, the MSHE of the RK, at the NSA at the Institute of Mathematics at OD53.12. on the topic: verification and automation of microcontroller programming, the dissertation is scientifically defended. (050010, Almaty, Pushkin St., house 125, office 306). Currently, she is associate professor of the Department of Space Technique And Technology at the L.N. Gumilyov ENU, Astana, Kazakhstan. Her research interests include IT technologies, radio engineering, programming of microcontrollers and automation systems, modern technologies for designing space nanosatellites. She can be contacted by email: moldamurat@yandex.kz.

Yerzhan Seitkulov professor of the Department of Information Security, IT Faculty at the Gumilyov ENU, Astana, Kazakhstan. He was born in the village of Karakastek and studied at the Physics and Mathematics Lyceum from 1993 to 1996. Graduated from the Faculty of Mechanics and Mathematics of Moscow State University. He is a nominated of the state prize in the "Science" category. Research interests - cryptography, coding theory, cloud computing, voice information protection, supercomputer technologies, distributed computing. He is also the head of a number of scientific and technical projects and programs through line ministries. Over the past 10 years, he has led 8 scientific projects in the field of information security. He can be contacted at email: yerzhan.seitkulov@gmail.com.

Sabyrzhan Atanov received a degree of bachelor in space radio communications from the MTUCI in 1979, a PhD in theoretical electrical engineering from the Moscow Power Engineering Institute in 1989, and in 2010 received a Doctor of Engineering degree in the specialty of mathematical, software support of computing machines, complexes and computer networks. He is currently a professor in the Department of CSE at Gumilyov ENU. He has experience in the development of robotic systems, programming in high- and low-level languages, and numerical modeling. He has a great deal of experience in the management of state budget projects and initiative research. For the past 5 years, he has been working on theoretical and practical issues of artificial intelligence. He has extensive experience with machine learning algorithms, pattern recognition, and microcontroller system design. He has published more than 30 scientific papers. He can be contacted at email: Atanov5@mail.ru.



Makhabbat Bakyt received her Bachelor of Engineering and Technology and Master of Engineering from the L.N. Gumilyov ENU, Astana, Kazakhstan. She is currently a doctoral student of the Department of Information Security, IT Faculty at the L.N. Gumilyov ENU. Her interests include next research area: aircraft data encryption, cryptographic protection, information security. She can be contacted at email: bakyt.makhabbat@gmail.com.

Banu Yergaliyeva she was born in the city of Arkalyk in 1985. She studied at the Faculty of Mathematics and Informatics of ENU. He is a master in the field of mathematical modeling of economics. Now, she is a doctoral student on the specialty information security, L.N. Gumilyov ENU, Astana, Kazakhstan. She is a leading researcher at the Scientific Institute of Information Security and Cryptology. Research interests applied cryptography, cloud technologies, internet of things, secure processing in the cloud, secure storage of big data in the cloud. She can be contacted at email: banu.yergaliyeva@gmail.com.