Linked System of Data Organization and Management

Serhii Kulibaba[1], Liudmyla Zubyk[1], Oleg Kurchenko[1], Igor Sinitsyn[2], and Nataliia Mazur[3]

[1]*Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv, 01601, Ukraine*
[2]*Institute of Software Systems of National Academy of Sciences of Ukraine, Akademika Glushkova ave. 40, Kyiv, 03187, Ukraine*
[3]*Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

This article presents a new method of cryptographic data encryption. The principle of operation consists of processing input data—changing the structure in a keyless format. There are a sufficient number of similar algorithms, which have the names symmetric and asymmetric. They work with keys for encryption or decryption. The new method will make it possible to process data according to the appropriate algorithm without changing the size of the input data, only by changing the structure, and also without using a key for decryption. For decryption, you need to apply the proposed algorithm in the reverse order. Currently, communication systems are gaining popularity, because society wants to maintain contact with others remotely, as well as with the security of personal data. The data loss of some systems has been noticed repeatedly, so in addition to displaying the new algorithm, the principle of data organization and management, which is called a "Linked System", will be displayed. A significant number of systems are closed. They use other methods to keep data confidential. In addition to saving data, data may also be transferred. Transmission is carried out through communication channels, namely certain protocols. Some systems use special communication protocols to connect clients to the server. Each protocol can have a different data structure. The principle of application of the algorithm does not depend on the very structure of the system on which the corresponding protocol works. The algorithm is applied to all data that can be transmitted over the network mesh to which the clients are connected. Thanks to the individual approach, it is possible to achieve data reliability, as well as avoid the use of device resources thanks to an optimized algorithm and some software development tools.

Keywords

System, encryption, decryption, key, protection, modification, speed

1. Introduction

Developers of various systems try to maintain data privacy and security. At the same time, decisions are made to use already existing cryptographic encryption methods from primary sources [1].

The state of confidentiality of some communication and other systems was investigated, and it was noticed that the necessary information of users was repeatedly obtained by attackers. Because the general structure and encryption algorithms are already known, the probability of obtaining data is an order of magnitude higher for criminals.

An individual approach is required to ensure data reliability. As an example, try to create your data processing algorithm, electronic digital signatures, and communication protocols, and apply them in centralized or other data organization systems that work on the appropriate communication to receive or transfer, or store data [2, 3].

In addition, various services that provide individual services use different systems of organization and data management. The choice of one or another system is individual for everyone. To find a balance between security and economy,

CPITS 2023: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: kulibseryyy@gmail.com (S. Kulibaba); zubyk.liudmyla@knu.ua (L. Zubyk); oleg.kurchenko@knu.ua (O. Kurchenko); ips2014@ukr.net (I. Sinitsyn); n.mazur@kubg.edu.ua (N. Mazur)
ORCID: 0000-0002-7316-1214 (S. Kulibaba); 0000-0002-2087-5379 (L. Zubyk); 0000-0002-3507-2392 (O. Kurchenko); 0000-0002-4120-0784 (I. Sinitsyn); 0000-0001-7671-8287 (N. Mazur)

it was decided to investigate the working principles of already known data organization algorithms and develop the newest one [4].

2. Analysis of Publications, the Status of the Issue, and the Statement of the Problem

2.1. Analysis of Research and Publications

Currently, there are several ways to organize data for any system. Among them, the following are known: centralized, decentralized, and distributed. Centralized can be suitable for use by any software, because the principles of data management are simple [5]. Decentralized is usually used to check data for validity and reliability [6]. Distributed ones work according to a similar principle of decentralized methods, but partially with the duplication of information on each server device to increase the fault tolerance of the system [7].

Data stored internally in operating and other systems consist of bytes. It can be called a standardized form of digital information. A byte is a certain length of a binary code, which is replaced by a symbol or a special symbol during encoding [8].

When creating your cryptographic encryption algorithm, you should take into account the properties: confidentiality, immutability, and source [9]. Confidentiality remains for all users of systems where an appropriate data protection method is used. Immutability indicates that the data sent to the system must not change so that the system itself has the opportunity to verify the source. The system user confirms the sent data.

There are enough cryptographic encryptions. They can be distinguished by signs—symmetric and asymmetric. Symmetric methods work only with a public key, which is called “public” [10, 11]. It can be sent with secure data so that the recipient can decipher the information [12]. In asymmetric methods, two keys are used—public and private [13]. The principle of operation is similar to symmetric, but with a modification—encryption with a public key, and decryption with a private key, and without announcing it externally in the system.

The change in the internal structure of the data occurs due to the change in the positions of symbols and special symbols that directly form the input data [14]. When using certain development tools, you can get the decimal value of a byte right away, where the replacement process is much more simplified [15].

2.2. Analysis of the State of the Issue in the Applied Field

For several years, the use of various methods of data organization has been necessary to use for the development of any online or offline platform. The prerequisite for this is the permanent storage or retrieval of data, where the appropriate technique helps to most effectively solve several issues.

Client-server architectures often use centralized methods. Services that require data security and verification, such as services with cryptographic currencies, use decentralized solutions. For high security and failure resistance of server devices, distributed methods of data organization are used.

Some popular companies use one of the existing methods. Centralized solutions were chosen by the developers of the well-known Instagram, Facebook, and Telegram tools. Decentralized was chosen by the developers of cryptographic currencies Bitcoin, and Etherium. Distributed methods used by Google in its search engine.

2.3. Formulation of the Problem

Each development company is looking for the most effective method of data organization, which will result in less equipment costs, support, and scaling. At the same time, high-quality customer service will be obtained.

After analyzing the existing methods and systems, no optimal solution was found among the existing ones, which would give fewer costs for device maintenance and provide sufficient computational efficiency, in particular, a sufficient level of data security.

3. Ways of Organizing and Managing Data

3.1. Centralized Systems

A few years ago, centralized systems were popular in creating a variety of applications.

A centralized system (center) is a way of organizing data that contains all information and

processes input data with a single device. Fig. 1 shows an example of data organization by centralizing them [16].

To create a centralized system, several software components need:

1. *Communication protocol*. For users of the corresponding system to be able to receive data, a certain protocol is used: TCP, FTP, UDP, etc.
2. *Database*. Since the protocols do not include data storage methods, a database is used to obtain preliminary information.

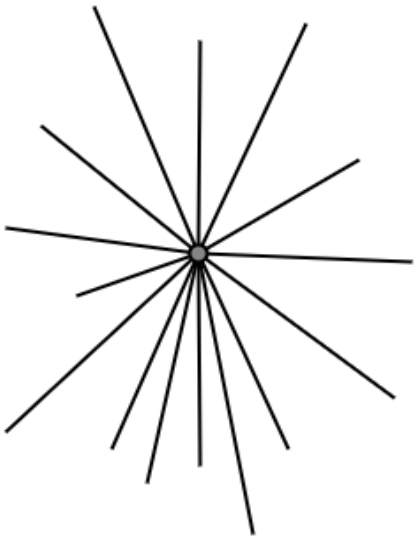

Figure 1: Centralized organization and management of data

Centralization is used by a sufficient number of applications, including web applications. This type of organization is less secure in terms of data storage, but at the same time, it is more economical. As an example, it is used by the famous application Instagram. While researching the possibility of "breaking" the system internally, several cases were observed, and the employees of this company needed to come to certain locations where the server devices are located and fix them.

By this we can say that the destruction of the entire system can occur by the destruction of one component of the system—the server device.

3.2. Decentralized Systems

After some time, in the 80s and 90s, the concept of a decentralized system appeared, followed by the methodology of creating decentralized systems.

A decentralized system is a set of blocks that contain certain data and increase their security level by hashing (each block) and verifying the validity of this data. Fig. 2 shows the principle of decentralized data organization [17].

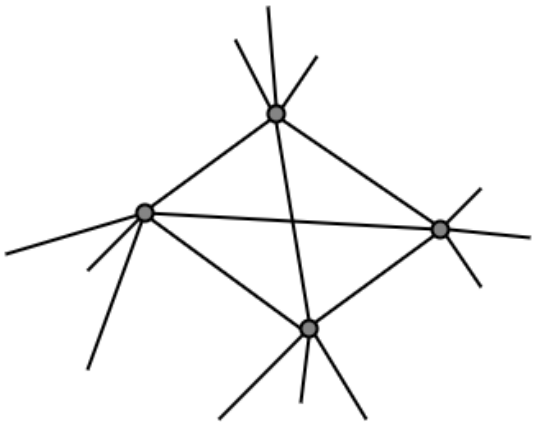

Figure 2: Decentralized organization of data

A hash function is a function that transforms input data of any length into a fixed length [18].

The requirements for the hash function are as follows:

1. Resistance of collisions
2. Resistance to finding the prototype
3. Resistance to the search for a second prototype.

Collisions. Collision resistance means that there is no algorithm for finding a collision in a short period. A collision is a situation where there is a pair of values that, by applying to the input of the function, you can get a valid result.

The first prototype. This is a requirement for a hash function where updating the initial data in an adequate amount of time is not possible.

The second prototype. The party that has the initial data and the corresponding hash value cannot create other data that will return the same result at the input of the hash function.

Similar systems contain data blocks. All blocks are interconnected, because each previous block is processed by a hash function, and data is transferred to the new block. This method of organization is called blockchain in decentralized systems. In this case, it is difficult to replace the data, because devices or a certain device are used, which contain all the data for further validation.

Validation occurs thanks to other devices that constantly compare their values with the server values—consensus.

Consensus is the validation of data by using a variety of methods. There are a sufficient number of data verification methods [19]:

1. Proof-of-Stake.
2. Proof-of-Work.
3. Delegated Proof-of-Stake.

All methods are based on proof, but some are based on work and luck. As an example, the Delegated Proof-of-Stake principle describes below:

1. *Delegate*. The user who controls governance in the blockchain.
2. *Validator*. Nodes that verify the correctness of the consensus.
3. *Witnesses* Users responsible for blockchain security and validation.

Cryptocurrencies usually use for decentralization.

3.3. Distributed Systems

A distributed system is a way of organizing data that distributes data across multiple server devices. Fig. 3 shows an example of data organization by distribution.

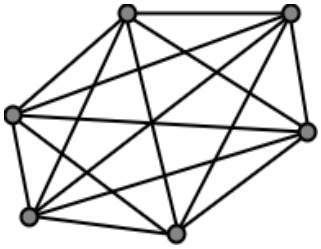

Figure 3: Distributed system

This type of organization also includes consensus. To receive, update, and delete data, voting takes place between existing server devices. Among them is the main device—the controller. When the control server is lost, a vote is taken to select a new control device [20].

Because some parts of the data can be stored not only on one device but also possibly on several. This causes high failure resistance in the system. But at the same time, the design and costs of such a system increase significantly, because not only data is distributed, but also hardware resources. As an example, the Google Chrome application is the largest distributed system in the world.

4. Linked System of Data Organization and Management

4.1. Structure and Principles of Work

A linked system is a way of organizing and managing data that divides data into N-parts (blocks) and distributes them across N-devices, without keeping duplicates. The recommended number of server devices for applying this data organization methodology is 3 or more. From a smaller number of devices, it makes no sense to build such a system, as well as a distributed or decentralized one.

Fig. 4 shows the principle of operation of the connected system.

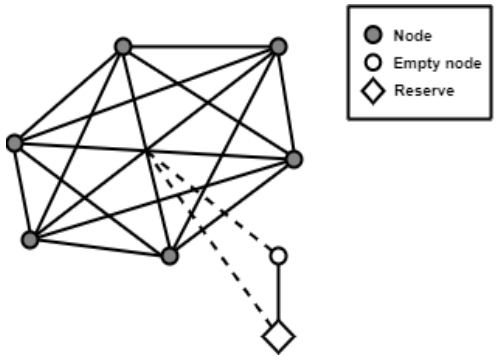

Figure 4: The principle of operation of the Linked system

To create and apply this system, it is necessary to decide on a conditional structure. There are 3 server devices (S1–S3), one "empty" (E) and one spare (R). A user is connected to S2 and is sending data. In this case, the program initially encrypts the data in an E2E (end-to-end) way, divides it into 3 parts, puts it in a queue, and sends it to all S. Thanks to the queue, the data transmission is synchronized, and does not need to use the computing power of other servers, until which the data gets, only the network load. All data that has been received must be sent to R via E at an appropriate frequency, where E signals R to open an individual communication channel for data transmission.

Assume that S2 has failed. Then the data will be received from R through E by opening a data channel. The R device serves to restore data if it has been lost so far, as well as to partially replace a non-working server. The system will work as long as at least 1 server is running. The idea of a backup server is just to be a container for data, and should not have a lot of computing power.

It may be that you need to scale the system. Then, after installing a new server device, data is transferred from the backup device to the new one:

$$\frac{1}{N+M}, \quad (1)$$

where N is the total number of servers, M is the number of new devices.

When the data wrote, other working servers continue to work, but only to receive users, without returning data from their database,

redirecting user requests to new servers. The database of previous servers is overwritten. Thanks to such processing, a certain number of users is not lost, but at the same time, there is a load on the network of new servers:

$$\frac{I\ ^{Mbit}/_{s}}{P}, \quad (2)$$

where I is the maximum speed of the Internet, P is the number of connected users (threads).

After summing up the likely scaling events of the associated system, it is possible to calculate the amount of memory that will be freed up when new devices are added (3).

$$\frac{\sum_{i}^{N} V_i}{N+M}\ (or)\ V_i, \quad (3)$$

where Vi is the amount of physical memory of the current device,
N is the number of devices,
M is the number of new devices.

4.2. Communication Methods Between Devices

There are a sufficient number of methods for organizing communication between devices. Among them, TCP/IP, UDP, FTP, HTTP, and others are used [21].

The corresponding protocol is used for the corresponding tasks. The TCP/IP protocol is in high demand in the design of client-server architectures. In addition, developing software using this protocol requires a minimum of system costs, so it was decided to choose this option.

TCP/IP (Transmission Control Protocol, Internet Protocol) is a network model of data transmission, which is presented in digital form. This model includes 4 stack levels [22]:

1. *Application level*. At this level, rules are defined, thanks to which data exchange will be carried out. For example, thanks to HTTP and FTP protocols.
2. *Transport level*. The transport layer helps to correctly organize the data for the recipient while maintaining sequences.
3. *Network layer*. The level that is intended for the transmission of data packets to the recipient, by calculating the network address based on the network mask.
4. *Channel level*. Describes how data is encoded for the transmission of data packets at the physical layer.

The interaction of devices in a connected system takes place at the network level because it is necessary to transfer relevant information to several devices while maintaining data security.

Data security can be maintained at the network level, because this level contains: identifier, flag, source address, destination address, parameters, data, etc. The way the data is addressed is defined, so only the data itself that needs to be transferred is processed. Data processing can be done in different ways, including the use of cryptographic encryption methods [23].

1.3. Comparative Analysis

To determine the quality of the proposed system, it was decided to compare it with all existing data management and organization systems.

Failure resistance:
a) Centralized—low
b) Decentralized—medium
c) Distributed—high
d) **Linked—high.**

Service*:*
a) Centralized—low
b) Decentralized—medium
c) Distributed—high
d) **Linked—high**

Scalability*:*
a) Centralized—low
b) Decentralized—medium
c) Distributed—high
d) **Linked—high.**

Development*:*
a) Centralized—high
b) Decentralized and Distributed—medium
c) **Linked—medium.**

Evolution:
a) Centralized—low
b) Decentralized—medium
c) Distributed—high
d) **Linked—high.**

You can compare and find the differences between distributed and connected systems:

1. *Safety*. Compared to a linked system, complete data is not stored on multiple servers. While the data of the linked system is stored on all available devices in blocks.

2. *Data storage*. Distributed systems duplicate data, as a result of which there is a high failure resistance to the loss of one or more servers. In a connected system, data is

divided into blocks and distributed on servers, where if one is lost, the backup can be replaced, but without using its computing power to receive users, only for data transmission.

3. *Costs and design*. A distributed system is difficult to design and particularly expensive. The related system will be less expensive due to the efficient use of memory when scaling (3), and at the same time, it is not difficult to design.
4. *The speed of receiving/returning data*. In a distributed system, the data has a complete form. Due to this, the speed will be lower compared to the related one, which has a block system of data storage.

5. Cryptographic Encryption Method Transposition Data Method

5.1. Signs of Cryptographic Encryptions

A symmetric cryptosystem is a way to increase the level of software protection by changing the data structure with a special unique key.

The key is a set of secret information, thanks to which the digital signature of the document and other data is verified.

The key is required to process the data structure for both encryption and decryption. The same key is required to process the same information. If the key is lost, it will not be possible to get complete information.

Asymmetric cryptosystems are a way of increasing the protection of software using an external and an internal key.

The foreign key is used in symmetric encryption methods. Internal—in asymmetrical ones. The difference between these types of encryption is the formation of two keys for encryption and decryption of data in asymmetric encryption.

The external key is available to all recipients of data, and the internal key is unique and is available to each recipient of information. These two keys help to decrypt fully protected information. The only drawback of the asymmetric type of encryption is the speed of processing [24].

5.2. Properties of cryptographic encryptions

Cryptographic encryption is the replacement of the data structure with symbols and the creation of a certain key to replace the symbols with the original structure. Encryption is used for three purposes:

1. *Privacy*. Thanks to cryptographic protection methods, information can be made inaccessible to persons trying to steal this information.
2. *Immutability*. Encrypted information cannot be tampered with during transmission or storage.
3. *Confirm the source*. Encrypted information has information about the sender.

Data exchange between users occurs as follows:

1. The original text, image, and video are transformed into an encrypted form with the help of an algorithm, and the recipient will have a special key to decrypt this data.
2. The encrypted message is sent to the recipient.

The receiver decrypts the message using a special key.

5.3. Properties of Data Recording in Operating Systems

The initial data can be different—bytes or text information. When receiving text information, it is necessary to convert it into bytes. A byte is a unit of storage and processing of digital information, which can have values from 0 to 256 for one character.

Some development tools can immediately convert symbols into bytes, while the processing process becomes automated, in particular, faster [25]. Because the data must be processed with bytes, the binary code or symbol must be converted to bytes for the systems to work properly (Table 1). If necessary, the data can be returned to the usual form—text—apply to decode (1).

$$\sum_{k=1}^{m} (n_{k-1} \times 2^{m-k})_{10} \quad (4)$$

Table 1
UTF-8 characters with binary and decimal values

Binary	Decimal	Symbol
00100001	33	!
00100010	34	“
00100011	35	#
00100011	49	1
00110001	57	9
01000000	64	@
01000001	65	A
01100010	98	b
01111110	126	~

5.4. Algorithm of Transposition Data Method

The TDM data processing algorithm is as follows:

1. Receiving input data and, if necessary, converting it to bytes.
2. Distribution of data into 6 parts with their processing with step 12:

a) Parts 1 and 2 with the initial processing position 0 carry out the replacement of the values N and N+1.

b) Parts 3 and 4 with processing start position 2 perform value substitution from N to N+2 and from N+2 to N+4.

c) Parts 5 and 6 with the initial processing position 6 carry out the substitution of values from N to N+3 and from N+3 to N+6.

3. Replacement of the first half of the original values with another.
4. Saving the result.

For decryption, it should be taken into account that the value of the length of the input encrypted data may not be even, therefore, at the beginning of the decryption, it is necessary to determine the percentage by dividing the length by 2 for further correctness of the result—permutation of halves. Then the decoding is in reverse order.

When using this approach, difficulties may arise with the processing of large data. As an example, 1GB can take a relatively long time to process. In this case, the input data should be divided into blocks that will process parts according to the same algorithm [26]. To obtain greater uniqueness of the placed data, at the end of processing, it is necessary to rearrange several parts, at most three, for large volumes.

5.5. Principles and Areas of Application

At the moment, communication systems are rapidly gaining popularity. In most of them, data security is determined by the use of cryptographic encryption methods. The processing of the data itself takes place thanks to certain algorithms on the input data of users. The data structure is a message. To use the proposed algorithm, you should convert text information into bytes, then apply the proposed or algorithm. Any data consists of bytes regardless of the system, so the flexibility of use lies in this, in particular the speed of processing.

Other closed systems process and transmit data via communication channels. Such systems use specific communication protocols to connect clients to the server. Each protocol may have a different data structure and operating principles. Regardless of the principle of operation and data structure, information processing can be carried out.

5.6. Comparison with Analogues

Currently, there are a sufficient number of algorithms for increasing the level of data protection: AES, DES, 3DES, and others. These methods are symmetrical [27]. The principle of their operation consists of encryption and decryption of data with a public key. There are also asymmetric methods. They work similarly to symmetric methods but have a private key, which is used for decryption and is not announced outside the system.

Both symmetric and asymmetric algorithms have drawbacks. Symmetric encryption methods use a single key to encrypt and decrypt data. This contributes to a greater probability of receiving valid data from the attacker. Asymmetric algorithms solve the problem using a single key. But in this case, more computing power is needed to process the data before obtaining their proper appearance [28, 29].

During the study of the performance of the TDM method, it was observed that unique values were obtained from the input. At the same time, it can be assumed that data security is at a high level. It can be assumed that a set of bytes of data can be defined by a single character of length N-characters of the same type. In this case, the attacker can more likely choose an algorithm to

decrypt the message. This assumption applies to known symmetric and asymmetric algorithms. Next, you can define the level of data security for all types of encryption:

1. No key method. The security level is sufficient.
2. Symmetric method. The security level is medium.
3. Asymmetric method. The security level is high.

This level of security is due to the openness of the digital sequence of values, namely keys, as well as the time spent to obtain valid data illegally.

6. Conclusion

This paper considered well-known methods of data organization and management, which are in demand among companies that develop or design a service delivery system.

During the analysis of all methods, it was decided to develop a new method of data organization and compare it with the existing ones. As it was shown, a system with its potential was obtained, with its evaluation according to the relevant criteria.

In addition, the principle of operation of the TDM method was displayed. Thanks to the individual approach to increasing the level of data protection, software developers have the opportunity to create an individual method of data encryption.

No device resource usage was observed during the TDM method development study. This makes it possible to apply the algorithm on most devices that need to save computing power for computing other data.

Currently, communication systems are gaining popularity in society. Therefore, a decision was made to create our communication system and use a data processing algorithm. The algorithm made it possible to increase the level of data protection on the users' devices themselves without using the resources of the server and their own devices. Thanks to this, conditional attackers will have a lower probability of obtaining valid data due to an individual approach to increasing the reliability of personal information.

7. References

[1] S. Gnatyuk, et al, New Secure Block Cipher for Critical Applications: Design, Implementation, Speed and Security Analysis, Advances in Intelligent Systems and Computing, vol. 1126 (2020) 93–104. doi: 10.1007/978-3-030-39162-1_9

[2] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/picst54195.2021.9772181

[3] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

[4] M. Vladymyrenko, et al., Analysis of Implementation Results of the Distributed Access Control System. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (2019). doi: 10.1109/picst47496.2019.9061376

[5] S. Lupin, H. Linn, K. Nay Zaw Linn, Data Structure and Simulation of the Centralized Control System for Transport Robots, 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019, 1880–188. doi: 10.1109/EIConRus.2019.8656853

[6] T. Nowak, M. Suriyah, T. Leibfried, Power Tracking in a MMC-multi-terminal HVDC System with Centralized and Decentralized MPC Using a Black Box Modeling Approach, 2017 52nd International Universities Power Engineering Conference (UPEC), 2017, 1–4. doi: 10.1109/UPEC.2017.8232017

[7] M. Sader, et al., Distributed Fuzzy Fault-tolerant Consensus of Leader-follower Multi-Agent Systems with Mismatched Uncertainties, J. Systs. Eng. Electrons. 32(5) (2021) 1031–1040. doi: 10.23919/JSEE.2021.000088

[8] M. Sharma, D. Somwanshi, Improvement in Homomorphic Encryption Algorithm with Elliptic Curve Cryptography and OTP Technique, 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), 2018, 1–6. doi: 10.1109/ICRAIE.2018.8710434

[9] S. Kulibaba, O. Kurchenko, Cryptographic Method of Pattern Reverse Multiplication Data Encryption, Cybersecur. Educ. Sci. Technol. 3(15) (2022) 216–223.

[10] H. Comon-Lundh, V. Cortier, E. Zalinescu, Deciding Security Properties for Cryptographic Protocols. Application to

Key Cycles, 2010. 1–42. doi: 10.1145/1656242.1656244

[11] J. Gitanjali, et al., ASCIi Based Cryptography Using Unique Id, Matrix Multiplication and Palindrome Number, The 2014 International Symposium on Networks, Computers and Communications, 2014, 1–3. doi: 10.1109/SNCC.2014.6866509

[12] T. Zaw, M. Thant, S. Bezzateev, Database Security with AES Encryption, Elliptic Curve Encryption and Signature, 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), 2019, 1–6. doi: 10.1109/WECONF.2019.8840125

[13] L. Yu, Z. Wang, W. Wang, The Application of Hybrid Encryption Algorithm in Software Security, 2012 Fourth International Conference on Computational Intelligence and Communication Networks, 2012, pp. 762–765. doi: 10.1109/CICN.2012.195

[14] N. B. Rad and H. Shah-Hosseini, GBHE: Grid-Based Cryptography with AES Algorithm, 2008 International Conference on Computer and Electrical Engineering, 2008, 185–189. doi: 10.1109/ICCEE.2008.36

[15] K. Rajeshwaran, K. Anil Kumar, Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function, 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2019, 1–6. doi: 10.1109/ICECCT.2019.8869146

[16] Working Group on Centralized Substation Protection and Control, IEEE Power System Relaying Committee, Advancements in Centralized Protection and Control Within a Substation, IEEE Transactions on Power Delivery, 31(4) (2016) 1945–1952. doi: 10.1109/TPWRD.2016.2528958

[17] R. Ben Amor, S. Elloumi, Decentralized Model Reference Adaptive Control for Interconnected Robotic Systems, 2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2017, 235–240. doi: 10.1109/STA.2017.8314907

[18] K. Rajeshwaran, K. Anil Kumar, Cellular Automata Based Hashing Algorithm (CABHA) for Strong Cryptographic Hash Function, 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2019, 1–6. doi: 10.1109/ICECCT.2019.8869146

[19] J. Jayabalan, J. N, A Study on Distributed Consensus Protocols and Algorithms: The Backbone of Blockchain Networks, 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, 1–10. doi: 10.1109/ICCCI50826.2021.9402318

[20] T. Castiglia, C. Goldberg, S. Patterson, A Hierarchical Model for Fast Distributed Consensus in Dynamic Networks, 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), 2020, 1189–1190. doi: 10.1109/ICDCS47774.2020.00137

[21] J. A. R. P. de Carvalho, et al., A Contribution to Performance Measurements of IEEE 802.11 A, B, G Laboratory WEP Point-To-Point Links Using TCP, UDP and FTP, 2010 International Conference on Applied Electronics, 2010, 1–5.

[22] M. Ruiz, et al., Limago: An FPGA-Based Open-Source 100 GbE TCP/IP Stack, 2019 29th International Conference on Field Programmable Logic and Applications (FPL), 2019, 286–292. doi: 10.1109/FPL.2019.00053

[23] A. Djama, B. Djamaa, M. Senouci, TCP/IP and ICN Networking Technologies for the Internet of Things: A Comparative Study, 2019 International Conference on Networking and Advanced Systems (ICNAS), 2019, 1–6. doi: 10.1109/ICNAS.2019.8807890

[24] T.Huang, F.Guo, Research on Single Sign-on Technology for Educational Administration Information Service Platform, 2021 3rd International Conference on Computer Communication and the Internet (ICCCI), 2021, 69–72. doi:10.1109/ICCCI51764.2021.9486813

[25] C. Lin, et al., Research on Key-bytes Encryption Technology of SDH Channel, 2020 International Conference on Robots & Intelligent System (ICRIS), 2020, 207–209. doi: 10.1109/ICRIS52159.2020.00059

[26] M. Alam, W. Badawy, G. Jullien, A Novel Pipelined Threads Architecture for AES Encryption Algorithm, IEEE International Conference on Application-Specific

Systems, Architectures, and Processors, 2002, 296–302. doi: 10.1109/ASAP.2002.1030728

[27] R. Teodorescu, et al., Virtual Instrumentation Application for Symmetrical and Asymmetrical Text Encryption/Decryption Studying, 2015 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2015, 23–26. doi: 10.1109/ECAI.2015.7301245

[28] C.-F. Wu, et al., Benchmarking Dynamic Searchable Symmetric Encryption with Search Pattern Hiding, 2019 International Conference on Intelligent Computing and its Emerging Applications (ICEA), 2019, 65–69. doi: 10.1109/ICEA.2019.8858302

[29] S. Bonde, U. Bhadade, Analysis of Encryption Algorithms (RSA, SRNN and 2 Key Pair) for Information Security, 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2017, 1–5. doi: 10.1109/ICCUBEA.2017.8463720