AuSDiDe: Towards a New Authentication System for Distributed and Decentralized Structure based on Shamir's Secret Sharing

Omar SEFRAOUI[1], Afaf Bouzidi[2], Kamal Ghoumid[3]
National School of Applied Sciences
Engineering Sciences Laboratory LSI
Oujda, Morocco

El Miloud Ar-Reyouchi[4]
Department of Telecommunication and Computer
Science, Abdelmalek Essaadi University
Tétouan, Morocco

***Abstract*—Nowadays, connected devices are growing exponentially; their produced data traffic has increased unprecedentedly. Information systems security and cybersecurity are critical because data typically contain sensitive personal information, requiring high data protection. An authentication system manages and controls access to this data allowing the system to ensure the legitimacy of the access request. Most of the current identification and authentication systems are based on a centralized architecture. However, some concepts as Cloud computing and Blockchain use respectively distributed and decentralized architectures. Users without a central server will own platforms and applications of the next generation of Internet and Web3. This paper proposes AuSDiDe, a new authentication system for the distributed and decentralized structure. This solution aims to divide and share keys toward different and distributed nodes. The main objective of AuSDiDe is to securely store and manage passwords, private keys, and authentication based on the Shamir secret sharing algorithm. This new proposal significantly reinforces data protection in information security.**

Keywords*—*Shamir's secret sharing; authentication system; decentralized; distributed; blockchain

I. Introduction

Currently, the number of connected machines is growing exponentially. This is explained by several factors such as the use of social networks, streaming and sharing videos, online services (payment, purchases, etc.), connected objects, cryptocurrency [1].

The world has never been digitized as it is today. Digitization of different services, the use of cryptocurrency, IoT, etc. Moreover, the Covid-19 pandemic has given a boost to digitization, paving the way for new opportunities for growth, competitiveness and inclusion. The global data traffic has increased at an unprecedented rate over the last decade. There are various challenges and issues associated with this data.

Among these challenges, security and privacy have been considered as important issues since data often involves different types of sensitive personal information, e.g., addresses, personal preference, banking details, governmental data , financial, medical, military, or NFT's - Non-fungible token. Putting the data on the Net and on the Cloud [2] makes them vulnerable. This requires more vigilance from the administrators and owner of this data. To put more reliable and secure means to protect and secure the data against malicious people and botnets. It is necessary to choose the security criteria to be taken into account. Commonly used security criteria are availability, integrity, and confidentiality, but it may be relevant to add others such as proof, control, anonymity, reliability. The scale of needs will be determined according to these security criteria. Information systems security and cybersecurity ensure data protection. An authentication system manages and controls access to this data [3]. Fig. 1, 2, and 3 show a centralized, decentralized, and distributed organizational structure.

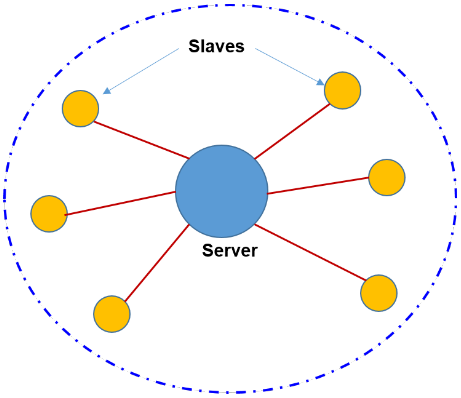

Fig. 1. Centralized Organizational Structure.

In Fig. 1, server systems with one or more slave nodes directly linked to a central server are centralized systems. In many companies, this is the most frequent sort of system.

In Fig. 2, every node in a decentralized system makes its own choice. The sum of the individual node choices determines the system's ultimate behavior. It is worth noting that the request is not received and responded to by a single organization structure.

A distributed system shown in Fig. 3 comprises a group of loosely coupled processors that are linked together via a communication network. A distributed system may consist of computational and diverse nodes connected by a communication network. Any node's total resources should be visible and freely available to other nodes. The choice of a load sharing or global planning technique is an important aspect of a distributed system's design configuration.

The advantage of the proposed approach, on the contrary

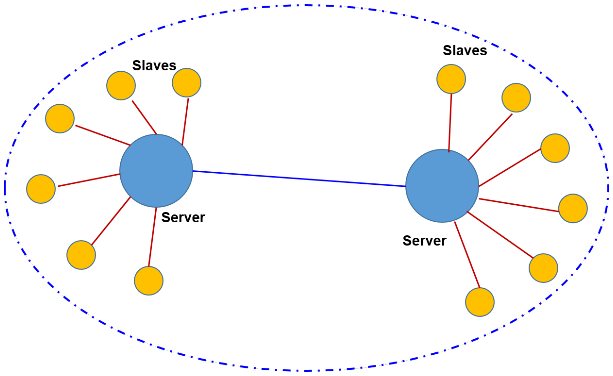

Fig. 2. Decentralized Organizational Structure.

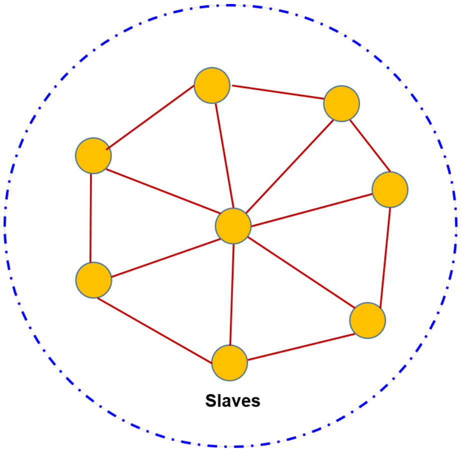

Fig. 3. Distributed Organizational Structure.

to most traditional secret sharing schemes, is that the shares are distributed and decentralized. This study presents a novel authentication scheme for the distributed (Fig. 3)and decentralized (Fig. 2) structure. This method aims to split and share keys across several remote nodes.

Most of the current identification and authentication systems are based on centralized architecture [4], today it is necessary to think about new methods and structures in order to strengthen the authentication and to be compatible with the new architectures.

There are some concept like Cloud computing [5] and Blockchain [6] use respectively distributed and decentralized architectures [7] as shown in Fig. 2 and 3. For example, in the next generation Internet, the platforms and applications built on the Web3 will be owned by users, without a central server [8]. In order to remedy these limitations and security concerns, this paper present a new approach, focused on the authentication systems, key and password management.

In docker, integrity comes from trust, i.e. the user decides to retrieve a docker image from the docker hub, which is a set of community images. Docker security relates to threats and attacks that challenge security based on confidentiality, integrity, and availability of services.The application system must function flawlessly during the expected use ranges and guarantee access to the services and resources installed with the expected response time. Basic docker provides functionality to have high availability, Docker Swarm, an orchestrator that allows you to manage your cluster of containers.Indeed, the security of the information system is considered one of the primary issues to be established. Each organization must define a security policy to succumb to its needs and protect these resources and their trade secrets.

In order to increase the level of security [9], a new authentication mechanism is introduced. This authentication mechanism for distributed and decentralized structures is based on Shamir's secret sharing.

Hadoop is a big data processing paradigm that can efficiently address the issues of big data because of its distributed storage and parallel processing properties, as well as other benefits such as open source. The proposal is considered as the last method to guarantee the robustness of any key management system is to divide the keys into various bits, as recommended in the Split Keys approach. In this approach, no one individual has access to the real key; instead, the key must be used by a group of people. The system suggested in this paper splits and distributed keys to distinct and scattered nodes in all clusters.

AuSDiDe a new proposed architecture to securely manage passwords, private key and authentication. Shamir's algorithm is used to share secret information

The main purpose of this system is to split the secret key into parts, giving each server its own shared key, where some or all of the parts are needed in order to rebuild a passphrase that gives access to the secret.

The remainder of the paper is laid out as follows. First a review of the related work realized in this topic is presented. Then a presentation of the architecture of an authentication system. After the implementation results are displayed. The conclusions and future work are presented in the last Section.

II. Related Work

Nowadays, there are many proposals for securing and managing authentication system. The proposed system reinforces security, prevents certain attacks such as man in the middle, identity theft, and adapts to new distributed and decentralized architecture.

To improve the security of keys used for encryption, [10] proposes a threshold secret sharing system employing Newton division difference interpolating polynomial in a distributed Cloud context.

The study [11] proposes a system that employs secure multiparty computation (SMPC) protocols with Shamir secret sharing for password- and iris-based authentication.

Hashing may not be able to hide data as effective in post quantum era [12], an authentication protocol which will use Shamir's secret sharing method to authenticate with server is proposed. A novel approach based on blockchain technology [13], digital signatures and threshold ElGamal Cryptosystem to address the problem of single point of failure.

The authors in [14] provide a viable way for protecting the traditional password-based authentication system since this sort of authentication is often required. They suggest a way for sharing a secret based on Shamir's well-known (k, n) threshold approach.

In [15], the authors discuss a new approach for managing the secrets in a decentralised way by leveraging decentralised identity concepts such as verifiable credential technologies, password-authenticated key exchange protocols and multi-party computation.

Another approach were developed in [16] who introduce PASSAT is a practical method that enhances the security assurance provided by today's cloud architecture without needing any modifications or collaboration from cloud service providers. PASSAT is a cloud-invisible program that enables users to safely and effectively save and retrieve their files on public cloud storage with a single master password.

III. Shamir's Secret Sharing

Authentication for a computer system is a process that allows the system to verify the legitimacy of the access request. The system then assigns this entity the identity data for this session. Access to the resources of an information system by an entity is broken down into three sub-processes, authentication, identification and access control [17].

Cryptography is one of the disciplines of cryptology focusing on protecting messages ensuring confidentiality, authenticity and integrity by often using secrets or keys. Shamir's Secret Sharing is an example of this cryptographic algorithm [18].

A. Distributed Scenario

A distributed system is a computer environment in which numerous nodes on a network are used to distribute different components [7].

Because distributed networks are formed up of equal, interconnected nodes, data ownership, and computing resources are dispersed equitably throughout the network.These nodes divided up the work and coordinated their efforts to finish the assignment more quickly than if it had been assigned to a single node. Compared to decentralized networks, distributed networks are more scalable.

A node in a distributed network may fail on its own without impacting the rest of the system. It is more difficult to change information on a distributed network since data is spread equitably throughout the whole network [7].

B. Decentralized

Decentralization is defined by the distribution of powers. Scaling decentralized networks is simple. Instead of depending on a single central node, a decentralized network spreads information processing among numerous nodes [7]. Even if one of the master nodes fails, the remaining servers can continue to offer data access to users, and the network as a whole will keep running. Because information kept on the network is spread across numerous points rather than via a single one, decentralized networks provide a higher level of consumer privacy [19]. Furthermore, user requests are often completed faster when using a decentralized network. Fig. 4 shows the nodes of the AuSDiDe node's topology.

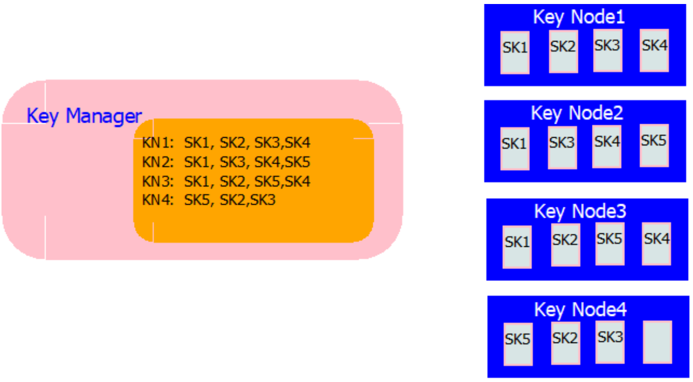

Fig. 4. AuSDiDe Nodes.

Fig. 5 details a schematic diagram of the general AuSDiDe architecture used for Distributed and Decentralized Structure Based on Shamir's Secret Sharing.

C. Shamir's Secret-Sharing Scheme

Shamir's Insider Information Adi Shamir is the creator of sharing. A secret is split into pieces in a kind of dispersed secret [18]. Each participant has their own shared key, where some or all the parts are needed to reconstruct a passphrase. Shamir's secret sharing or key sharing, is a process which a private encryption key is split into separate fragments. Every fragment is useless, unless it is sufficiently assembled to reconstitute the original key [7].

It is not necessary that all the participants reconstitute the access password. This is why the threshold scheme is sometimes used where a number k of the parts is sufficient for rebuild the original secret [20].

In Shamir's secret-sharing arrangement, there are n shareholders [21]. $U_i = \left\{U_1, U_2, ..., U_n\right\}$ and a mutually trusted dealer D.

The dealer D produces $a(t-1)$ degree polynomial $f(x) \in Z_p$, where P is a prime integer, to divide the secret S into n shares. $S = f(0)$ is the shared secret, and before sending the (x_i, y_i) to the shareholder U_i the dealer calculates the secret-sharing shares as y_i = f(x$_i$) for $x_i \neq$0.

When regenerating the secret, at least t shares (x_i, y_i) are required to recover the polynomial $f'(x)$, allowing each shareholder to get the secret $S = f'(0)$. The approach is comprised of two algorithms: secret reconstruction and share generation [21]:

For share generation, the $(t-1)$ degree polynomial is defined as:

$$f(x_i) = a_0 + a_1 x^1 + a x^2 + ... + a_{t-1} x^{t-1}, (mod\ p) \qquad (1)$$

and $a_i \in Z_p$, for $0 \leq i \leq t-1, a_{t-1} \neq 0$,the secret $S = f(0) = a_0$.

In $a(t, n)$ secret-sharing system, n points arer randomly chosen as $x_i : 1 \leq i \leq n$, and $x_i \neq 0 \in Z_p$,, the

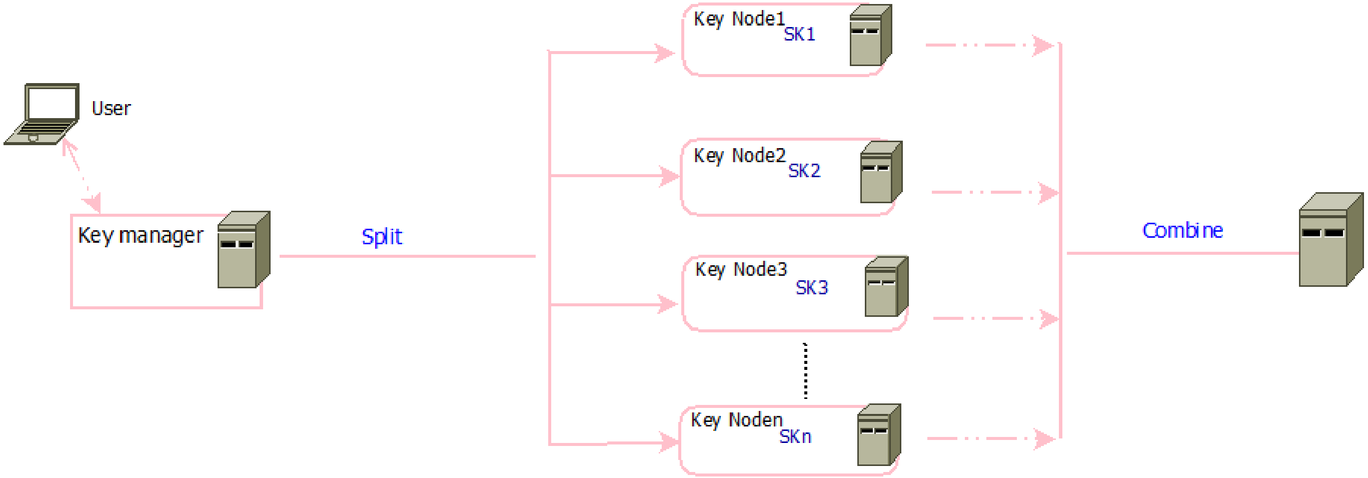

Fig. 5. Architecture AuSDiDe.

dealer calculates $y_i = f(x)$ and transmits $s_i = (x_i, y_i)$ to shareholders U_i.

For a secret reconstruction [18], supposing that t shareholders $U_1, U_2, ..., U_t$. Each shareholder U_i gives a share s_i to the other stockholders. After that, if a shareholder possesses m shares $s_1, s_2, ..., s_m$, he may retrieve $f'(x)$ using the Lagrange interpolation polynomial as [21]:

$$f'(x) = \sum_{i=1}^{t} s_i \prod_{j=1, i \neq j}^{t} \frac{x_j - x}{x_j - x_i}, (mod\ p) \tag{2}$$

The secret S will be computed as:

$$f'(0) = \sum_{i=1}^{t} s_i \prod_{j=1, i \neq j}^{t} \frac{x_j}{x_j - x_i}, (mod\ p) \tag{3}$$

IV. AuSDiDe General Architecture

The AuSDiDE is introduced to enhance security and been developed to increase the level of security. This system takes into consideration those architectures: distributed and centralized.

AuSDiDe is compsed of nodes playing different exclusive roles between them. Hacking and attacking servers should be difficult. Getting a key will not be enough to encrypt the passphrase, you need to get all shared keys. It will be complicated, given the number of servers.

The AuSDiDe is composed of two main Node as shown in Fig. 4: Key Manager – the master and Key Node – the slave. One of the machines is the master, called Key Manager: This machine contains all names and key parts, like a phone book.

All other machines are Key Node. They store the different shared secret key. The key Manager knows where the keys are, which part of the key and on which key Manager are registered.

The key manager will be dividing the secret into several parts – (n, k) key parts after having defined the threshold k. As illustrated in Fig. 5, this task called split operation.

The threshold represents the minimum number of parties necessary to reconstitute the passphrase and unlock access to the secret. This task called combine operation.

V. Implementation

In this section, the implementation of the AuSDiDe is presented. The created cluster is composed of different servers, playing different exclusive roles. For this operation, the docker [22] and Hadoop framework [23] are used.

A. Docker Security Advantages

Docker's most widely used containerization technique can raise the degree of security if used correctly (in comparison to running applications directly on the host). On the other hand, misconfigurations might result in a reduction in security or even the introduction of new vulnerabilities. Docker gives the ability to automate the deployment of applications into Containers [24]. Docker offers an additional layer of deployment engine on top of a Container environment where programs are virtualized and executed. Docker is meant to offer a speedy and lightweight environment in which code may be executed quickly and an additional facility of the competent work process to remove the code from the computer for testing before production [24]. You may certainly start with a docker with a basic configuration system, a docker binary with a Linux kernel. Docker has four major internal components: Docker Server and Client, Docker Registries, Docker Images, and Containers. A Docker image is used to generate a Docker container [22]. Containers store all of the components needed for a program, allowing it to execute in isolation. Assume there is an image of Ubuntu OS with MongoDB server; when executed with the docker run command, a container is produced, and MongoDB server is operating on Ubuntu OS [22].

B. Benefits and Advantages of Hadoop

The Apache Hadoop project creates open-source software for scalable, distributed computing. The software library is a framework that enables the distributed processing of massive data volumes across computer clusters by using basic programming techniques [23]. It is intended to grow from a single server to thousands of computers, providing local computing and storage.

Rather than relying on hardware to provide high availability, the library is intended to identify and manage failures at the application layer, allowing a highly available service to be delivered on top of a cluster of machines that may all fail [23].Therefore, it is widely used today to store, analyze, and manipulate huge amounts of data: Hadoop is a standard for Big Data processing. Hadoop refers to its ecosystem and all software such as Apache Spark, Cloudera Impala, Sqoop, etc.

The Experimental Architecture of AuSDiDe Implementation is illustrated in Fig. 6.

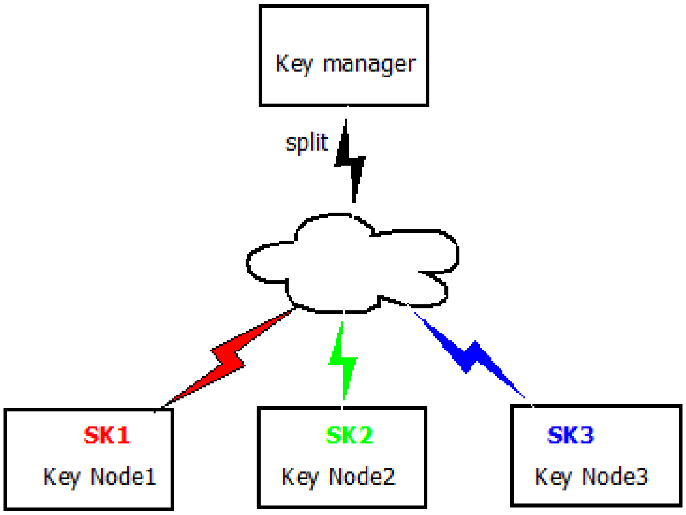

Fig. 6. Experimental Architecture of AuSDiDe Implementation.

The three containers represent a Key Manager and three Key nodes utilizing a Docker image. We use throughout the implementation three containers, representing respectively a Key Manager and three Key Nodes using docker image [24], as shown in Fig. 6.

The result of this execution shows how the split operation at the Key Manager was able to divide and share the shared keys SK1, SK2 and SK3 and store them to the different Key Node1, Key Node2 and Key Node3.

For the inverse operation i.e combine operation, the threshold equal two, representing the minimum number of parties necessary to reconstitute the passphrase and unlock access to the secret. It can be SK1 and SK2; SK2 and SK3 or SK1 and SK3.

VI. Discussion

Several considerations must be taken to determine the authentication system adapted for new architectures. The future of internet (for example web 3.0) implement a decentralized architecture, all machines can play the role of master and slave at the same time. For example, Peer-to-peer (P2P) is a model of computer network structured in a decentralized way [25], the communications between nodes with equal responsibility. In the world network, nodes are identified by a logical IP address. To maintain anonymity in a network, it is better to use private or public key addresses. These different constraints have been well studied for the development of the AusDiDe solution.

VII. Conclusion

This paper proposes a new approach focused on authentication systems, private keys, and password management. This solution presents a new way of thinking about authentication systems and sensitive data security. These will be adapted to future generation Internet, e.g., web3. The implementation of AuSDiDe clearly shows better security and an obstacle for malicious attacks. The AuSDiDe system divides and shares keys toward different and distributed nodes in all clusters. Hacking requires obtaining all the shared keys, making it difficult for hackers. As continuity to this work and to enhance the AuSDiDe functionality, the artificial intelligence concept will develop an intelligent AuSDiDe system operating in decentralized and hybrid architecture as Blockchain. Towards a framework for a smart AuSDiDe with a learning system to anticipate intrusions and anomalies in order to reinforce security.

References

[1] BERDIK, David, OTOUM, Safa, SCHMIDT, Nikolas, et al. A survey on blockchain for information systems management and security. Information Processing and Management, 2021, vol. 58, no 1, p. 102397.

[2] YANG, Caixia, TAN, Liang, SHI, Na, et al. AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. IEEE Access, 2020, vol. 8, p. 70604-70615.

[3] SHARMA, Uttam, TOMAR, Pradeep, ALI, Syed Sadaf, et al. Optimized Authentication System with High Security and Privacy. Electronics, 2021, vol. 10, no 4, p. 458.

[4] JEONG, Junho, KIM, Donghyo, IHM, Sun-Young, et al. Multilateral Personal Portfolio Authentication System Based on Hyperledger Fabric. ACM Transactions on Internet Technology (TOIT), 2021, vol. 21, no 1, p. 1-17.

[5] KRISHNARAJ, N., BELLAM, Kiranmai, SIVAKUMAR, B., et al. The Future of Cloud Computing: Blockchain-Based Decentralized Cloud/Fog Solutions–Challenges, Opportunities, and Standards. In : Blockchain Security in Cloud Computing. Springer, Cham, 2022. p. 207-226.

[6] GAI, Keke, GUO, Jinnan, ZHU, Liehuang, et al. Blockchain meets cloud computing: A survey. IEEE Communications Surveys and Tutorials, 2020, vol. 22, no 3, p. 2009-2030.

[7] VERGNE, J. P. Decentralized vs. distributed organization: Blockchain, machine learning and the future of the digital platform. Organization Theory, 2020, vol. 1, no 4, p. 2631787720977052.

[8] ZARRIN, Javad, PHANG, Hao Wen, SAHEER, Lakshmi Babu, et al. Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Computing, 2021, p. 1-26.

[9] MASLOUHI, Imane, GHOUMID, Kamal, ZAIDOUNI, Jamal, et al. Network Higher Security of Intelligent Networks Platforms in Telecommunications Areas. In : Proceedings of the Mediterranean Conference on Information and Communication Technologies 2015. Springer, Cham, 2016. p. 225-233.

[10] FATIMA, Shahin et AHMAD, Shish. Secure and effective key management using secret sharing schemes in cloud computing. International Journal of e-Collaboration (IJeC), 2020, vol. 16, no 1, p. 1-15.

[11] FĂLĂMAŞ, Diana-Elena, MARTON, Kinga, et SUCIU, Alin. Assessment of Two Privacy Preserving Authentication Methods Using Secure Multiparty Computation Based on Secret Sharing. Symmetry, 2021, vol. 13, no 5, p. 894.

[12] GUPTA, Kishor Datta, RAHMAN, Md Lutfar, DASGUPTA, Dipankar, et al. Shamir's Secret Sharing for Authentication without Reconstructing Password. In : 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2020. p. 0958-0963.

[13] HENA, M. et JEYANTHI, N. Blockchain Based Authentication Framework for Kerberos Enabled Hadoop Clusters. In : Soft Computing for Problem Solving. Springer, Singapore, 2021. p. 315-327.

[14] BISSOLI, Andrea et D'AMORE, Fabrizio. Authentication as a service: Shamir Secret Sharing with byzantine components. arXiv preprint arXiv:1806.07291, 2018.

[15] JAROUCHEH, Zakwan et ÁLVAREZ, Iván Abellán. Secretation: Toward a Decentralised Identity and Verifiable Credentials Based Scalable and Decentralised Secret Management Solution. In : 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2021. p. 1-9.

[16] SATVAT, Kiavash, SHIRVANIAN, Maliheh, et SAXENA, Nitesh. PASSAT: Single Password Authenticated Secret-Shared Intrusion-Tolerant Storage with Server Transparency. arXiv preprint arXiv:2102.13607, 2021.

[17] ESPOSITO, Christian, FICCO, Massimo, et GUPTA, Brij Bhooshan. Blockchain-based authentication and authorization for smart city applications. Information Processing and Management, 2021, vol. 58, no 2, p. 102468.

[18] DZURENDA, Petr, RICCI, Sara, MARQUÉS, Raúl Casanova, et al. Secret Sharing-based Authenticated Key Agreement Protocol. In : The 16th International Conference on Availability, Reliability and Security. 2021. p. 1-10.

[19] BHATTACHARJEE, Arpan, BADSHA, Shahriar, SHAHID, Abdur R., et al. Block-phasor: A decentralized blockchain framework to enhance security of synchrophasor. In : 2020 IEEE Kansas Power and Energy Conference (KPEC). IEEE, 2020. p. 1-6.

[20] SAROSH, Parsa, PARAH, Shabir A., et BHAT, Ghulam Mohiuddin. Utilization of secret sharing technology for secure communication: a state-of-the-art review. Multimedia Tools and Applications, 2021, vol. 80, no 1, p. 517-541.

[21] LI, Guojia et YOU, Lin. A Consortium Blockchain Wallet Scheme Based on Dual-Threshold Key Sharing. Symmetry, 2021, vol. 13, no 8, p. 1444.

[22] RAD, Babak Bashari, BHATTI, Harrison John, et AHMADI, Mohammad. An introduction to docker and analysis of its performance. International Journal of Computer Science and Network Security (IJCSNS), 2017, vol. 17, no 3, p. 228.

[23] The Apache Hadoop project.URL: https://hadoop.apache.org/. access on Dec. 2021

[24] AHMED SHAIKH, Kasam et AGASKAR, Shailesh S. Containers and Azure Kubernetes Services. In : Azure Kubernetes Services with Microservices. Apress, Berkeley, CA, 2022. p. 103-129.

[25] KUSHWAHA, Satpal Singh, JOSHI, Sandeep, SINGH, Dilbag, et al. Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. IEEE Access, 2022.