УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2022 Том 22 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2022 Vol. 22 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2022-22-2-355-363

Whirlpool Hash Mutual Biometric Serpent Authentication (WPHMBSA) for secured data access in cloud environment

Krishnan Mohana Prabha[1]✉, Perumal Raja Vidhya Saraswathi[2], Saminathan Balamurali[3]

[1,2,3] Kalasalingam Academy of Research and Education, Tamil Nadu, 626126, India

[1] kmohanaprabha@gmail.com✉, https://orcid.org/0000-0001-8874-030X
[2] vidhyasaraswathi.p@gmail.com, https://orcid.org/0000-0001-5273-9067
[3] sbmurali@gmail.com, https://orcid.org/0000-0002-3010-245X

Abstract

Cloud systems allow data sharing capabilities for providing several benefits to users and organizations. However, authentication accuracy (AA) was not improved, and time consumption was not reduced. To increase authentication accuracy, Whirlpool Hash Mutual Biometric Serpent Authentication (WPHMBSA) Technique is designed to access data on a server in a secured manner. During the registration process, users' data are registered and stored on the server. After registering, the cloud server generates an ID and password for every registered user. For authentication, the user needs to login with an ID and password to the cloud server. During authentication, WPHMBSA Technique authenticates the biometric keys of the users. When a user is legitimate, WPHMBSA Technique confirms their authenticity to the server. Experimental evaluation of the WPHMBSA Technique and existing methods are performed by various parameters with the amount of cloud user's information. The experimental results show that the WPHMBSA Technique obtains high accuracy and confidentiality rate within minimum time.

Keywords

cloud systems, data sharing, registration, authentication, ciphertext, cloud services, cloud

For citation: Mohana Prabha K., Vidhya Saraswathi P.R., Balamurali S. Whirlpool Hash Mutual Biometric Serpent Authentication (WPHMBSA) for secured data access in cloud environment. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2022, vol. 22, no. 2, pp. 355–363. doi: 10.17586/2226-1494-2022-22-2-355-363

УДК 004.7

Взаимная биометрическая аутентификация для защищенного доступа к данным в облачной среде

Кришнан Мохана Прабха[1]✉, Перумал Раджа Видхья Сарасвати[2], Сарасвати Баламурали[3]

[1,2,3] Академия исследований и образования Каласалингама, Тамилнанд, 626126, Индия

[1] kmohanaprabha@gmail.com✉, https://orcid.org/0000-0001-8874-030X
[2] vidhyasaraswathi.p@gmail.com, https://orcid.org/0000-0001-5273-9067
[3] sbmurali@gmail.com, https://orcid.org/0000-0002-3010-245X

Аннотация

Облачные системы позволяют обмениваться данными, предоставляя ряд преимуществ пользователям и организациям. Однако точность аутентификации недостаточна, а затраты времени остаются значительными. Технология взимной биометрической аутентификации WPHMBSA (Whirlpool Hash Mutual Biometric Serpent Authentication) предназначена для повышения точности аутентификации и безопасного доступа к данным сервера. В процессе регистрации данные пользователей фиксируются и сохраняются на сервере. Облачный сервер генерирует идентификатор и пароль для каждого зарегистрированного пользователя. Для аутентификации пользователю необходимо войти в систему с идентификатором и паролем на облачном сервере. Технология WPHMBSA аутентифицирует биометрические ключи пользователей. В случае если пользователь зарегистрирован, WPHMBSA подтверждает его подлинность на сервере. Проведена экспериментальная оценка методики WPHMBSA в сравнении с существующими методами с использованием объема информации о

пользователе на сервере. Экспериментальные результаты показали, что метод WPHMBSA обеспечивает высокую точность и уровень конфиденциальности при минимальном времени аутентификации.

Ключевые слова
облачные системы, обмен данными, регистрация, аутентификация, зашифрованный текст, сервисы, облачный сервер

Ссылка для цитирования: Мохана Прабха К., Видхья Сарасвати П.Р., Баламурали С. Взаимная биометрическая аутентификация для защищенного доступа к данным в облачной среде // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 2. С. 355–363 (на англ. яз). doi: 10.17586/2226-1494-2022-22-2-355-363

Introduction

Cloud computing (CC) is a complicated system that includes different devices which support services. CC produces a flexible and convenient way for data access, which brings a variety of profits for mutual society and individuals. To distribute the optimum resource utilization, CC employs a large cluster that manages resources which are dynamically reconfigured. CC comprises different types of configurable distributed systems with connectivity and usage. CC is a paradigm that gives a massive computation capacity and enormous memory space at a low cost and thus brings great convenience to cloud users while using various services provided via CC and cloud storage service. But the existing authentication method may be failed to access the data in a secure manner. In order to overcome the issue, the Whirlpool Hash Mutual Biometric Serpent Authentication (WPHMBSA) Technique is introduced to secure cloud data access within minimum time. The main aim of the WPHMBSA Technique is to store cloud user data with a higher confidentiality rate and the minimum time complexity.

In order to overcome the existing issues, a novel WPHMBSA.Technique is introduced with the following contributions, WPHMBSA Technique is designed for data access from a server in a secured way. The registration phase, authentication phase, and data sharing phase are performed by the WPHMBSA Technique. To minimize the time complexity, the novelty of the Whirlpool hashing function is used in the WPHMBSA Technique. Whirlpool hashing function is used to register clients with their user details and then store them on the cloud server. Through the registration process, the server is provided with the ID and the password of the user. To increase the security and data confidentiality level in the cloud environment, the novelty of Mutual Biometric Key Authentication is employed to Authentication Server (AS), to carry out authentication in WPHMBSA Technique, when user sending needs to access data. To improve the cloud data access lesser time, the novelties of biometric keys of the users are applied in WPHMBSA Technique. This technique authenticates the biometric keys of the users. While the user is valid, WPHMBSA Technique proves its authenticity to the server. Symmetric keys and transmissions of the ciphertext to the cloud server are used by WPHMBSA Technique encrypting the user data. To secure the cloud data access lesser time, the novelty of Serpent Symmetric Secured Data Sharing is employed in WPHMBSA Technique. This technique permits the user to obtain the necessary services. WPHMBSA Technique doesn't allow users to access.

Related works

A biometrics-based authentication scheme was designed in [1] to deploy multi-cloud-server. But the AA was not improved by a biometrics-based authentication scheme. The SADS-Cloud architecture was introduced in [2] with three processes. SADS-Cloud of AA was not improved.

RS-IBE is introduced in [3] to present forward/backwards protection through user revocation functionalities and updates at the same time. RS-IBE of Authentication Time (AT) was not reduced. An efficient protocol was introduced in [4] without accessing secret keys for several users to permit query database and to decrypt retrieved results. However, data confidentiality was not reduced by the efficient protocol. In the cloud, authentication, access management, security, and services problems were reviewed in [5]. The designed model of AT is not minimal. A flexible framework is developed in [6] to produce the confidential sharing analysis among collaborators. However, the confidentiality level was not improved by a flexible framework.

A secure data sharing scheme was introduced in mobile devices in CC [7]. The designed scheme performed integrity verification to avoid incorrect computation. An improved biometric-based multi-server authentication scheme was introduced in [8] with an elliptic curve cryptosystem. The biometric-based multi-server authentication scheme was not reduced by the computational complexity. Selective end-to-end data-sharing was carried out in [9] through joining plans as proxy re-encryption and editable signature. However, AA was not reduced also. Attribute-based encryption (ABE) is carried out in [10] to protect and to make flexible control of the shared data. ABE of time complexity was not reduced.

An attribute-based data sharing scheme is presented in [11] to resource-limited mobile users in the cloud. Attribute-based data sharing scheme of security level was not reduced. To urban data sharing, an attribute-based cryptography system was designed in [12]. However, the data-sharing time was not reduced by an attribute-based cryptography scheme. An efficient approach was introduced in [13] with higher data protection and confidentiality with no data hiding. The main objective was used for compressing images through a lossy image coder. Fuzzy Conditional Broadcast Proxy Re-Encryption (FC-BPRE) was designed in [14] with a semi-honest proxy to convert the delegator's ciphertext into new ciphertext. However, the error rate was not reduced by FC-BPRE.

Based on a hybrid mechanism and symmetric encryption scheme, a generic attribute-based data sharing system was designed in [15]. Though computation cost

was reduced, the time consumption was not reduced by the Ciphertextpolicy attribute-based encryption (CP-ABE) scheme. Location verification protocol, called Ears, was designed in [16] to prevent distance frauds in the Cyber-Physical Systems (CPS) environment. Location verification protocol of time consumption was not minimized.

A blockchain-based distributed authentication method and network construction was constructed in [17]. Data confidentiality level was not reduced by the designed method. Certificateless Privacy Preserving Public Auditing (CLPPPA) method was introduced in [18] for sharing data with a collection of user revocation. However, the AA was not improved by the CLPPPA scheme. To maintain several users in public clouds, a traceable group data sharing scheme was introduced in [19]. But traceable group data sharing scheme of data sharing time consumption was not minimized. To dynamic user groups, secure fine-grained access control and data sharing scheme was introduced in [20]. The designed scheme of computational complexity was not reduced also.

Methodology

The WPHMBSA Technique is designed for enhancing cloud data access within a minimal time. WH-WPHMBSA technique comprised Whirlpool Hash Function (WPHF) and Mutual Biometric Serpent Authentication. WPHMBSA Technique performs authentication among users and servers. WPHF is employed in the WPHMBSA Technique because it generates the 512-bit hash value for any user data in the minimal time.

In Fig. 1, the WPHMBSA Technique performs secured data access in the cloud. Initially, users transfer requests to a server. An AS performs a biometric key verification process for every user request. AS performs the mutual biometric serpent authentication in the cloud environment. Whenever identity is correct, the cloud server provides the requested services to the equivalent user included. Hence, the WPHMBSA Technique increases the security and data confidentiality level in a cloud environment. WPHMBSA Technique comprises three processes: Registration, Authentication, and Data Sharing.

Registration

During the authentication process, a user has to register their personal details to access cloud data. WPHMBSA Technique is used at the registration phase to record the users' personal information on the cloud server. WPHF is used in the WHMBSA Technique to enhance the user information that is securely stored on the cloud server. WPF is a cryptographic hash function. WPHF is a compression tool with Advanced Encryption Standard. WPHF considers the data of any size as input and returns the 512-bit hash value. For every input user details of any size, WPHF generates the unique 512-bit hash value and stores it in the database. This helps the WHMBSA technique to secure the user data with lesser memory consumption. Below, the diagrammatic representation of the registration process using WHMBSA Technique is involved.

Fig. 2 illustrates the registration process in WPHMBSA Technique. As illustrated in the above figure, the user's personal information is transmitted to a server. Next, the cloud server produces a 512-bit hash value with the help of WPHF and stores it in the database to increase the data confidentiality level during the cloud access control process. After storing the user information in a secured manner, WPHMBSA Technique generates the user ID and key pair for each user who needs the cloud services. With generated user ID and key pair, WPHMBSA Technique improves the authentication performance of users compared with state-of-the-art works.

In WPHMBSA Technique, the cloud user named as and their details are symbolized as $CloudU_i = CloudU_1$, $CloudU$, …, $CloudU_n$ and their detalis are symbolized as $UserD_j = UserD_1$, $UserD_2$, … $UserD_m$ where m is the total number of user personal data. WPHMBSA Technique uses WPHF to produce the hash value for every user-entered data. The diagrammatic representation of WPHF is illustrated in Fig. 3.

Fig. 3 illustrates the WPHF process in WPHMBSA Technique. As described in the figure, WPHF considers

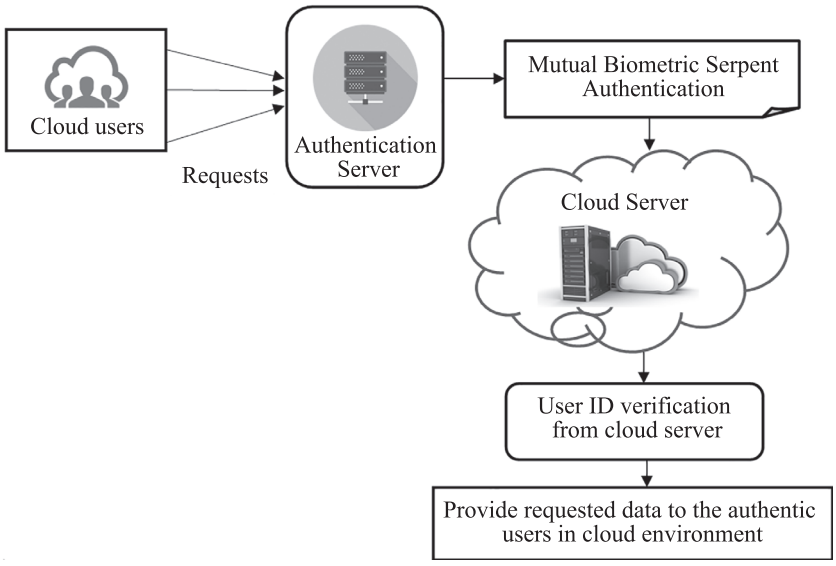

Fig. 1. Architectural diagram of WPHMBSA Technique for secured cloud data sharing

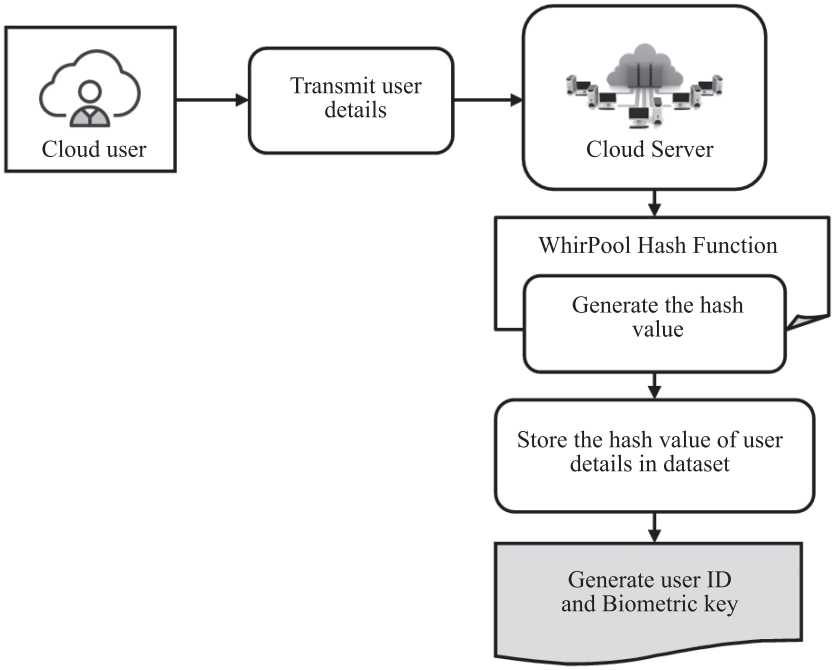

Fig. 2. Registration process

the user details $UserD_j$ as input; the output is the constant length string (512-bit hash value). After that, the cloud server stores the constructed hash value in the database and prevents the user details from malicious access. From that, WPHMBSA Technique increases the data confidentiality level in the cloud environment. In addition, the generated hash values consume lesser memory space than user details size. Therefore, WPHMBSA Technique attains the minimal time complexity for performing the secured data access control.

WPructs is the hash value for every input user details. It is created as

$$Hash = WHF(UserD). \quad (1)$$

In (1), *WHF* is the Whirlpool hash function, and '*UserD*' is the user details. *Hash* is the hash value of the user data. After finishing the registration process, the cloud server generates the user ID $User_{id}$ and key pairs to every user. The process is

$$CloudServer \rightarrow (User_{id}, Keypairs_i) \quad (2)$$

In (2), $Keypairs_i$ are the key pairs. For every cloud user, the server provides a unique ID and key pairs to secure access data on a cloud server. WPHMBSA Technique increases the authentication performance to identify the authentic user on the cloud server by user ID and key pairs.

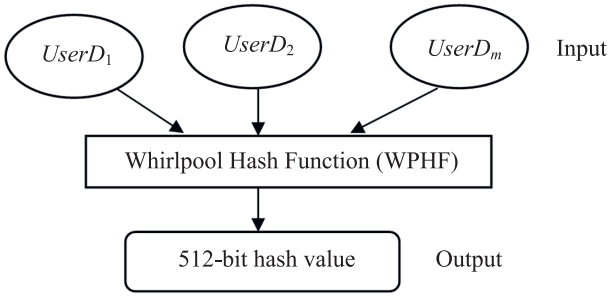

Fig. 3. Block diagram of Whirlpool hash function

Mutual Biometric Key Authentication

AS performs authentication in WPHMBSA Technique, while user sends requests to access data. When the user transmits a request to a server, AS asks for user ID $User_{id}$ and biometric keys BK_i. The user sends their user ID and biometric keys to the AS. AS authenticates whether the user is an authenticated user or not. AS verifies the user identity who wants to access the data in the cloud. WPHMBSA Technique allows only authentic users to access the data. Therefore, WPHMBSA Technique increases the security and data confidentiality level in the cloud environment.

Fig. 4 illustrates the mutual biometric authentication through an AS. As you can see in the above figure, the AS asks for user ID and biometric keys when they require cloud services. The cloud user enters the ID and biometric keys to the AS. AS authenticates user-personality through matching biometric key with the corresponding ID. The process looks like

$$AuthenticationServer \leftarrow E(User_{id}, BK_i)$$
$$AuthenticationServer = \begin{cases} BK_i = BK_i^*; \ Authenticated\ User \\ BK_i \neq BK_i^*; \ Unauthorized\ User \end{cases}. \quad (3)$$

In equation (3), BK_i is the biometric key, BK_i^* is the reference of the biometric key. When the user biometric key is matched with the equivalent ID, and the key is stored in the cloud server database, then the user is authorized or not. After the authentication process, AS identifies the user as an authenticated user and prove their identity to one another on the cloud server.

Serpent Symmetric Secured Data Sharing

When the user has been authenticated, the cloud server allows the user to obtain the requested data services.

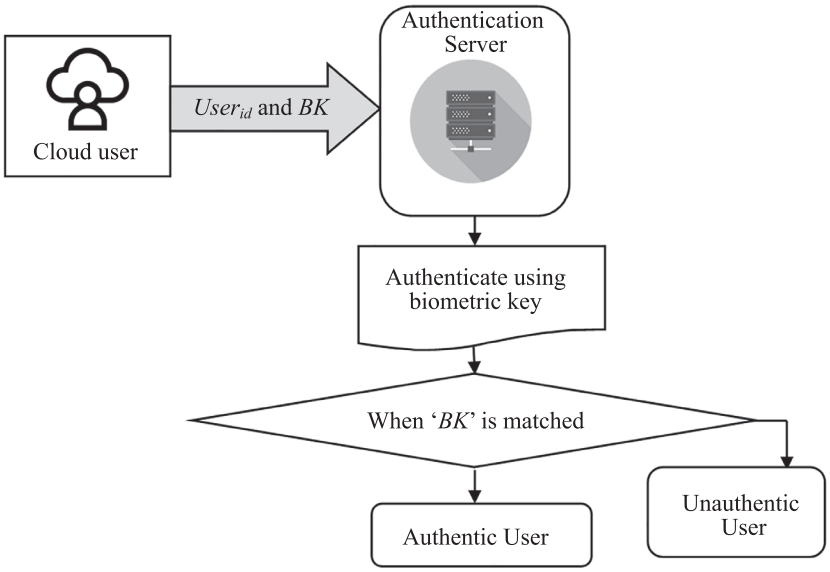

Fig. 4. Mutual biometric authentication process

The serpent is a symmetric key block cipher used in WPHMBSA Technique. The serpent has 128 bits and a supported key size of 128 or 256 bits. Cipher is a 32-round substitution–permutation network functioning on 32-bit words. Serpent Symmetric Key (SSK) algorithm employs two processes: *encryption* and *decryption*. In the SSK algorithm, the sender is an AS, and the receiver is the cloud server. The encryption process uses the SSK algorithm presented in Fig. 5.

Fig. 5 shows the flow process of the encryption using the SSK algorithm. As illustrated in the figure, SSK algorithm encrypts the data as following

$$Cipher \rightarrow E(SSK, UserData). \quad (4)$$

In (4), E is the encryption operator, and SSK and $UserData$ are the two ones that represent the SSK. In the cloud, encrypted data is transferred to the user. Then, a user transmits their user ID and encrypted data to a server. With the help of the SSK, the server decrypts the user data. The decryption process using the SSK algorithm is illustrated in Fig. 6.

Fig. 6 shows the flow process of decryption using the SSK algorithm. As illustrated in the figure, the cloud server performs the decryption with the help of SSK algorithm as following

$$OriginalData \rightarrow D(SSK, CT). \quad (5)$$

In (5), D is the decryption operator, CT stands for the ciphertext, and SKK is the SSK algorithm. Finally, the cloud server verifies that the user identity $User_{id}$ is matched with a user ID $User'_{id}$ in decrypted data using the below expression,

$$CS = \begin{cases} if\ User_{id} = User'_{id},\ then\ CloudU_i\ is\ allowed \\ to\ access\ data\ otherwise,\ CloudU_i \\ is\ not\ allowed\ to\ access\ data \end{cases}.$$

When two cloud user IDs are the same, the cloud server provides the required data services to the cloud user, $CloudU_i$. When the two-cloud user ID is not the same, the cloud server declines the service to the user in the cloud environment. Accordingly, WPHMBSA Technique achieves higher security for data access in the cloud environment with minimal time complexity. In this way, WPHMBSA Technique gives improved performance in CC. The WPHMBSA Technique step process is given below.

Following is WPHMBSA Algorithm 1.
// WhirlPool Hash Mutual Biometric Serpent Authentication
Input: Number of cloud users '$CloudU = CloudU_1, CloudU_2, \ldots CloudU_n$',
Output: Performed secured data access
Step 1: ***Begin***
Step 2: ***for*** each user $CloudU_i$
Step 3: ***for*** each user details $UserD_j$
Step 4: Generate hash value
Step 5: Store hash value in cloud server database
Step 6: Cloud server provides the $User_{id}$ and SSK to user
Step 7: ***end for***
Step 8: ***for*** user login with U_{id} and BK_i
Step 9: ***if*** $BK_i = BK_i^*$ ***then***

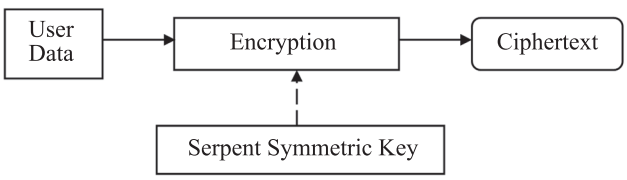

Fig. 5. Encryption using serpent Symmetric Key Algorithm

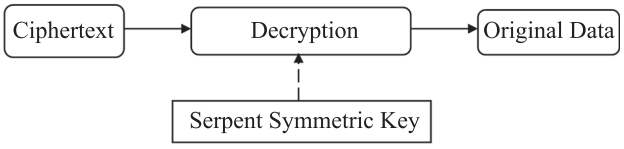

Fig. 6. Decryption using serpent Symmetric Key Algorithm

Step 10: User is an authenticated user
Step 11: ***else***
Step 12: User is an unauthenticated user
Step 13: ***endif***
Step 14: AS grants the permission to the user
Step 15: Encrypt data using SSK
Step 16: AS transmits Cipher to user
Step 17: User sent Ciphr and $User_{id}$ and *SSK* to the cloud server
Step 18: Cloud server decrypts the data with *SSK*
Step 19: ***if*** $(User_{id} = User'_{id})$ ***then***
Step 20: User allowed to access data
Step 21: ***else***
Step 22: User not allowed to access data
Step 23: ***endif***
Step 24: ***end for***
Step 25: ***end for***
Step 26: ***end***

In the above Algorithm 1, the process of the WPHMBSA Technique is used to obtain improved security during data access control. Whirlpool Hash-Based Double-DES Symmetric Key Kerberos Authentication (WH-DSKKA) Technique includes three main processes. Through the registration process, WPHMBSA Technique stores every user's personal information in the cloud server database by generating the hash value. During authentication, WPHMBSA Technique authenticates the biometric keys of the users.

If a user is legitimate one, WPHMBSA Technique confirms their authenticity to the server. WPHMBSA Technique encrypts user data using symmetric keys and transmits the ciphertext to the server. On the receiver side, the server decrypts user data shared by the sender. If the identity of the user is identical, WPHMBSA Technique permits the user to get needed cloud services. Otherwise, WPHMBSA Technique doesn't allow users to access cloud information. Finally, WPHMBSA Technique improves cloud data access lesser time.

Experimental Evaluation

Experimental evaluations of the proposed WPHMBSA Technique, existing biometrics-based authentication scheme [1], and SADS-Cloud architecture [2] are developed in Java language. To evaluate the results of the proposed technique, Amazon Access Sample Dataset is carried out to conduct the experiments. A dataset is considered as a UCI machine learning repository[1]. The dataset is a sample of access provisioned in the company. To identify authorized users to access data, services, or resources from the cloud server, the dataset is used. Depending on the attribute information, secured access control is carried out with many users. The results and discussion are explained below.

Results and Discussion

In this section, the proposed WPHMBSA Technique, existing biometrics-based authentication scheme [1], and SADS-Cloud architecture [2] are to be explained. The proposed and existing methods are evaluated with three different parameters: accuracy, time, and confidentiality rate. The graphical representations of the proposed and existing methods are illustrated for enhancing the proposed technique with parameter values.

Impact of Authentication Accuracy

AA is the proportion of the number of cloud users that are rightly recognized as authenticated users versus the entire number of users. The AA-percentage is used for the performance evaluation as illustrated below.

Fig. 7 presents AA versus the number of users. AA results of the WPHMBSA Technique are compared with the existing Biometrics-based authentication scheme [1] and SADS-Cloud architecture [2]. The authorized and unauthorized users are identified through the biometric authentication. During the registration process, the user's data are registered and stored on the server using the hash function. The hash value preserves the data from unauthorized user access. The AS authenticates the user using a biometric key. With symmetric keys, the Serpent algorithm is used for the encryption and decryption process for enhancing protection. The cloud server grants the services to the authorized user and denies services to unauthorized users. The authorized user accesses the cloud data to improve AA. WPBSA technique of AA is

[1] Available at: https://archive.ics.uci.edu/ml/datasets/Amazon+Access+Samples# (accessed: 10.02.2022).

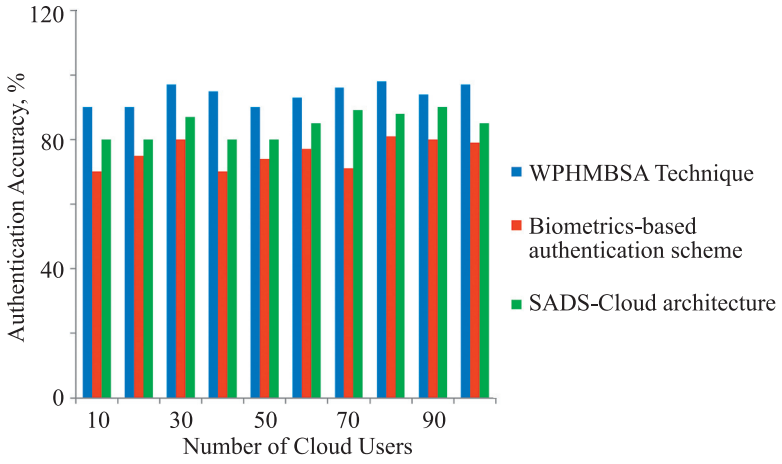

Fig. 7. Performance of Authentication Accuracy

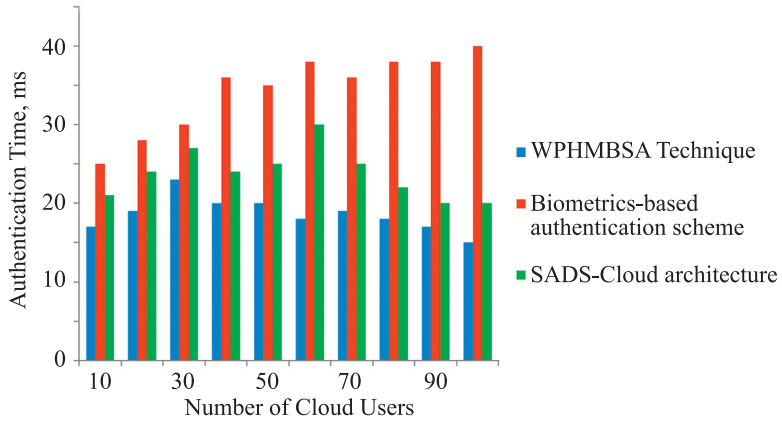

Fig. 8. Performance of Authentication Time

enhanced up to 24 % and 11 % compared with the existing Biometrics-based authentication schemes [1] and SADS-Cloud architecture [2], respectively.

Impact of Authentication Time

AT is the product of the number of times necessary for detecting authorized users and the number of cloud users. AT is determined in milliseconds.

Fig. 8 presents the performance results of AT versus the number of users. The AT of the WPHMBSA Technique is compared with the proposed WPHMBSA Technique and the existing Biometrics-based authentication scheme [1] and SADS-Cloud architecture [2]. For determining the AT, amount of cloud users is considered as input, ranging from 10 to 100. During the registration process, the user data is registered and stored on the server using hash function. Hash value protects data against unauthorized user access. To access data control in the company, an Amazon access sample dataset is used. Data has been accessed through the authorized user. The authorized and unauthorized users are identified through biometric authentication. The authorized user accesses the cloud data to reduce the time consumption during authentication. With the help of a biometric key, the AS validates the user. With symmetric keys, the Serpent algorithm is used for the encryption and decryption process for enhancing protection. The cloud server granted the services to the authorized user and denied the services to unauthorized users. The AT of the WPHMBSA Technique is considerably reduced by 45 % compared to the existing Biometrics-based authentication scheme [1] and 21 % compared to the existing SADS-Cloud architecture [2], respectively.

Impact of Confidentiality Rate

It is used to determine data from unauthorized users and accessed only by authorized users in the cloud. It is referred to as the proportion of the amount of data accessed by authorized users versus the entire amount of cloud data. The data confidentiality is determined by percentage. While the confidentiality rate is higher, the efficiency is increasing.

Fig. 9 presents the confidentiality rate versus the amount of data. The confidentiality rate results of the WPHMBSA Technique are compared with the existing Biometrics-based authentication scheme [1] and SADS-Cloud architecture [2]. For determining the confidentiality rate, the number of cloud users is considered as input, and it is ranged from 10 to 100. To access data control in the company, an Amazon access sample dataset is used. Data has been accessed through the authorized user. The authorized and unauthorized users are identified through biometric authentication. During the registration process, the user data is registered and stored on the server using a hash function. Hash value protects data against unauthorized user access. With the help of a biometric key, the AS validates the user. With symmetric keys, the Serpent algorithm is used for the encryption and decryption process for enhancing protection. Authorized user accesses cloud

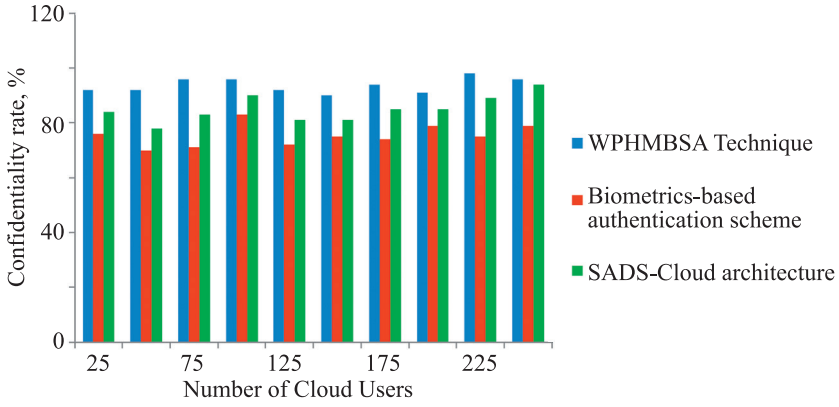

Fig. 9. Performance of confidentiality rate

data to increase the confidentiality rate. The confidentiality rate of the WPHMBSA Technique is enhanced by 25 % compared with the existing Biometrics-based authentication scheme [1] and by 10 % compared with the existing SADS-Cloud architecture [2], respectively.

Conclusion

A new technique called Whirlpool Hash Mutual Biometric Serpent Authentication (WPHMBSA) Technique is designed to access data on the server in a secured manner. During the registration process, the user data is registered and stored on the server using the Whirlpool hashing function. After registering, the cloud server generates an ID and password for every registered cloud user. The WPHMBSA Technique authenticates the user with the help of their biometric keys. When a user is legitimate one, WPHMBSA Technique confirms their authenticity to the server. The WPHMBSA Technique encrypts user data using symmetric keys and transmits the ciphertext to the server. On the receiver side, the server decrypts user data shared by the sender. If the identity of the user is equal, WPHMBSA Technique permits the user to get necessary cloud services. The WPHMBSA Technique enhances the protection of cloud data access with the minimal time complexity. The experimental result of the WPHMBSA Technique improves accuracy confidentiality rate and minimizes time compared with the existing methods. Therefore, WPHMBSA Technique is an efficient authentication mechanism to share data in cloud environments.

References

1. Kumari S., Li X., Wu F., Das A.K., Choo K.K.R., Shen J. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. *Future Generation Computer Systems*, 2017, vol. 68, pp. 320–330. https://doi.org/10.1016/j.future.2016.10.004
2. Narayanan U., Paul V., Joseph S. A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. *Journal of King Saud University — Computer and Information Sciences*, 2020, in press. https://doi.org/10.1016/j.jksuci.2020.05.005
3. Wei J., Liu W., Hu X. Secure data sharing in cloud computing using revocable-storage identity-based encryption. *IEEE Transactions on Cloud Computing*, 2016, vol. 6, no. 4, pp. 1136–1148. https://doi.org/10.1109/TCC.2016.2545668
4. Gahi Y., El Alaoui I. A secure multi-user database-as-a-service approach for cloud computing privacy. *Procedia Computer Science*, 2019, vol. 160, pp. 811–818. https://doi.org/10.1016/j.procs.2019.11.006
5. Indu I., Anand P.R., Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, 2018, vol. 21, no. 4, pp. 574–588. https://doi.org/10.1016/j.jestch.2018.05.010
6. Chadwick D.W., Fan W., Costantino G., De Lemos R., Di Cerbo F., Herwono I., Manea M., Mori P., Sajjad A., Wang X.S. A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Generation Computer Systems*, 2020, vol. 102, pp. 710–722. https://doi.org/10.1016/j.future.2019.06.026
7. Lu X., Pan Z., Xian H. An efficient and secure data sharing scheme for mobile devices in cloud computing. *Journal of Cloud Computing*, 2020, vol. 9, no. 1, pp. 60. https://doi.org/10.1186/s13677-020-00207-5
8. Wang F., Xu G., Wang C., Peng J. A provably secure biometrics-based authentication scheme for multiserver environment. *Security and Communication Networks*, 2019, pp. 2838615. https://doi.org/10.1155/2019/2838615
9. Hörandner F., Ramacher S., Roth S. Selective end-to-end data-sharing in the cloud. *Journal of Banking and Financial Technology*, 2020, vol. 4, no. 1, pp. 139–157. https://doi.org/10.1007/s42786-020-00017-y
10. Wei J., Huang X., Liu W., Hu X. Cost-effective and scalable data sharing in cloud storage using hierarchical attribute-based encryption with forward security. *International Journal of Foundations of Computer Science*, 2017, vol. 28, no. 7, pp. 843–868. https://doi.org/10.1142/S0129054117500289
11. Li J., Zhang Y., Chen X., Xiang Y. Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security*, 2018, vol. 72, pp. 1–12. https://doi.org/10.1016/j.cose.2017.08.007
12. Shen J., Liu D., Shen J., Liu Q., Sun X. A secure cloud-assisted urban data sharing framework for ubiquitous-cities. *Pervasive and Mobile Computing*, 2017, vol. 41, pp. 219–230. https://doi.org/10.1016/j.pmcj.2017.03.013
13. Khelifi F., Brahimi T., Han J., Li X. Secure and privacy-preserving data sharing in the cloud based on lossless image coding. *Signal*

Литература

1. Kumari S., Li X., Wu F., Das A.K., Choo K.K.R., Shen J. Design of a provably secure biometrics-based multi-cloud-server authentication scheme // Future Generation Computer Systems. 2017. V. 68. P. 320–330. https://doi.org/10.1016/j.future.2016.10.004
2. Narayanan U., Paul V., Joseph S. A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment // Journal of King Saud University — Computer and Information Sciences. 2020. in press. https://doi.org/10.1016/j.jksuci.2020.05.005
3. Wei J., Liu W., Hu X. Secure data sharing in cloud computing using revocable-storage identity-based encryption // IEEE Transactions on Cloud Computing. 2016. V. 6. N 4. P. 1136–1148. https://doi.org/10.1109/TCC.2016.2545668
4. Gahi Y., El Alaoui I. A secure multi-user database-as-a-service approach for cloud computing privacy // Procedia Computer Science. 2019. V. 160. P. 811–818. https://doi.org/10.1016/j.procs.2019.11.006
5. Indu I., Anand P.R., Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges // Engineering Science and Technology, an International Journal. 2018. V. 21. N 4. P. 574–588. https://doi.org/10.1016/j.jestch.2018.05.010
6. Chadwick D.W., Fan W., Costantino G., De Lemos R., Di Cerbo F., Herwono I., Manea M., Mori P., Sajjad A., Wang X.S. A cloud-edge based data security architecture for sharing and analysing cyber threat information // Future Generation Computer Systems. 2020. V. 102. P. 710–722. https://doi.org/10.1016/j.future.2019.06.026
7. Lu X., Pan Z., Xian H. An efficient and secure data sharing scheme for mobile devices in cloud computing // Journal of Cloud Computing. 2020. V. 9. N 1. P. 60. https://doi.org/10.1186/s13677-020-00207-5
8. Wang F., Xu G., Wang C., Peng J. A provably secure biometrics-based authentication scheme for multiserver environment // Security and Communication Networks. 2019. P. 2838615. https://doi.org/10.1155/2019/2838615
9. Hörandner F., Ramacher S., Roth S. Selective end-to-end data-sharing in the cloud // Journal of Banking and Financial Technology. 2020. V. 4. N 1. P. 139–157. https://doi.org/10.1007/s42786-020-00017-y
10. Wei J., Huang X., Liu W., Hu X. Cost-effective and scalable data sharing in cloud storage using hierarchical attribute-based encryption with forward security // International Journal of Foundations of Computer Science. 2017. V. 28. N 7. P. 843–868. https://doi.org/10.1142/S0129054117500289
11. Li J., Zhang Y., Chen X., Xiang Y. Secure attribute-based data sharing for resource-limited users in cloud computing // Computers & Security. 2018. V. 72. P. 1–12. https://doi.org/10.1016/j.cose.2017.08.007
12. Shen J., Liu D., Shen J., Liu Q., Sun X. A secure cloud-assisted urban data sharing framework for ubiquitous-cities // Pervasive and Mobile Computing. 2017. V. 41. P. 219–230. https://doi.org/10.1016/j.pmcj.2017.03.013
13. Khelifi F., Brahimi T., Han J., Li X. Secure and privacy-preserving data sharing in the cloud based on lossless image coding // Signal Processing. 2018. V. 148. P. 91–101. https://doi.org/10.1016/j.sigpro.2018.02.016

Processing, 2018, vol. 148, pp. 91–101. https://doi.org/10.1016/j.sigpro.2018.02.016
14. Fang L., Ge C., Huang Z., Wang J. Privacy preserving cloud data sharing system with flexible control. *Computers & Electrical Engineering*, 2018, vol. 70, pp. 978–986. https://doi.org/10.1016/j.compeleceng.2018.02.048
15. Zhang Y., Zheng D., Chen X., Li J., Li H. Efficient attribute-based data sharing in mobile clouds. *Pervasive and Mobile Computing*, 2016, vol. 28, pp. 135–149. https://doi.org/10.1016/j.pmcj.2015.06.009
16. Zhang Z., Chen X., Ma J., Shen J. SLDS: Secure and location-sensitive data sharing scheme for cloud-assisted Cyber-Physical Systems. *Future Generation Computer Systems*, 2020, vol. 108, pp. 1338–1349. https://doi.org/10.1016/j.future.2018.01.025
17. Singh C., Chauhan D., Deshmukh S.A., Vishnu S.S., Walia R. Medi-Block record: Secure data sharing using block chain technology. *Informatics in Medicine Unlocked*, 2021, vol. 24, pp. 100624. https://doi.org/10.1016/j.imu.2021.100624
18. Gudeme J.R., Pasupuleti S., Kandukuri R. Certificateless privacy preserving public auditing for dynamic shared data with group user revocation in cloud storage. *Journal of Parallel and Distributed Computing*, 2021, vol. 156, pp. 163–175. https://doi.org/10.1016/j.jpdc.2021.06.001
19. Shen J., Zhou T., Chen X., Li J., Susilo W. Anonymous and traceable group data sharing in cloud computing. *IEEE Transactions on Information Forensics and Security*, 2018, vol. 13, no. 4, pp. 912–925. https://doi.org/10.1109/TIFS.2017.2774439
20. Xu S., Yang G., Mu Y., Deng R.H. Secure fine-grained access control and data sharing for dynamic groups in the cloud. *IEEE Transactions on Information Forensics and Security*, 2018, vol. 13, no. 8, pp. 2101–2113. https://doi.org/10.1109/TIFS.2018.2810065

14. Fang L., Ge C., Huang Z., Wang J. Privacy preserving cloud data sharing system with flexible control // Computers & Electrical Engineering. 2018. V. 70. P. 978–986. https://doi.org/10.1016/j.compeleceng.2018.02.048
15. Zhang Y., Zheng D., Chen X., Li J., Li H. Efficient attribute-based data sharing in mobile clouds // Pervasive and Mobile Computing. 2016. V. 28. P. 135–149. https://doi.org/10.1016/j.pmcj.2015.06.009
16. Zhang Z., Chen X., Ma J., Shen J. SLDS: Secure and location-sensitive data sharing scheme for cloud-assisted Cyber-Physical Systems // Future Generation Computer Systems. 2020. V. 108. P. 1338–1349. https://doi.org/10.1016/j.future.2018.01.025
17. Singh C., Chauhan D., Deshmukh S.A., Vishnu S.S., Walia R. Medi-Block record: Secure data sharing using block chain technology // Informatics in Medicine Unlocked. 2021. V. 24. P. 100624. https://doi.org/10.1016/j.imu.2021.100624
18. Gudeme J.R., Pasupuleti S., Kandukuri R. Certificateless privacy preserving public auditing for dynamic shared data with group user revocation in cloud storage // Journal of Parallel and Distributed Computing. 2021. V. 156. P. 163–175. https://doi.org/10.1016/j.jpdc.2021.06.001
19. Shen J., Zhou T., Chen X., Li J., Susilo W. Anonymous and traceable group data sharing in cloud computing // IEEE Transactions on Information Forensics and Security. 2018. V. 13. N 4. P. 912–925. https://doi.org/10.1109/TIFS.2017.2774439
20. Xu S., Yang G., Mu Y., Deng R.H. Secure fine-grained access control and data sharing for dynamic groups in the cloud // IEEE Transactions on Information Forensics and Security. 2018. V. 13. N 8. P. 2101–2113. https://doi.org/10.1109/TIFS.2018.2810065

Authors

Krishnan Mohana Prabha — MCA, Research Scholar, Kalasalingam Academy of Research and Education, Tamil Nadu, 626126, India, SC 57321564100, https://orcid.org/0000-0001-8874-030X, kmohanaprabha@gmail.com
Perumal Raja Vidhya Saraswathi — PhD, Professor, Kalasalingam Academy of Research and Education, Tamil Nadu, 626126, India, SC 55357148700, https://orcid.org/0000-0001-5273-9067, vidhyasaraswathi.p@gmail.com
Balamurali Saminathan — PhD, Professor, Kalasalingam Academy of Research and Education, Tamil Nadu, 626126, India, SC 6602154096, https://orcid.org/0000-0002-3010-245X, sbmurali@gmail.com

Авторы

Мохана Прабха Кришнан — исследователь, Академия исследований и образования Каласалингама, Тамилнанд, 626126, Индия, SC 57321564100, https://orcid.org/0000-0001-8874-030X, kmohanaprabha@gmail.com
Видхья Сарасвати Перумал Раджа — PhD, профессор, Академия исследований и образования Каласалингама, Тамилнанд, 626126, Индия, SC 55357148700, https://orcid.org/0000-0001-5273-9067, vidhyasaraswathi.p@gmail.com
Баламурали Сарасвати — PhD, профессор, Академия исследований и образования Каласалингама, Тамилнанд, 626126, Индия, SC 6602154096, https://orcid.org/0000-0002-3010-245X, sbmurali@gmail.com

Received 09.09.2021
Approved after reviewing 09.02.2022
Accepted 17.03.2022

Статья поступила в редакцию 09.09.2021
Одобрена после рецензирования 09.02.2022
Принята к печати 17.03.2022