https://doi.org/ 10.33472/AFJBS.6.Si2.2024.2968-2977

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Optimized Profile Orient Blockchain Model for Improved Data Security in SOA and Cloud

Dr.Priya Vij, Associate Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India.
Mail ID:ku.priyavij@kalingauniversity.ac.in
ORCID ID: 0009-0005-4629-3413
Taruna Chopra, Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India.
Mail ID:ku.tarunachopra@kalingauniversity.ac.in
ORCID ID: 0009-0006-7910-6845

Article History

Volume 6,Issue Si2, 2024

Received:13 Apr 2024

Accepted : 05 May 2024

doi: 10.33472/AFJBS.6.Si2.2024. 2968-2977

Abstract:
The security in cloud data has been analyzed in detail where there exists number of approaches to secure the cloud data from different threats. Blockchain technique is the recent way of securing data from variety of threats. Number of approaches available with blockchain, which uses different encryption schemes and varies in the selection of key and scheme. However, the methods suffer to achieve higher security performance. To handle this issue, an Optimized Profile Orient Blockchain Model (OPOBM) is presented in this paper. The model classifies the users under various profiles and maintains set of key sets and scheme set for various profiles. Accordingly, an encryption scheme and key is identified as per the profile given and radical profile id. Using the radical profile id, the required encryption scheme and key are choose to encrypt the data. Also, unique hash code is produced for distinct blocks with radical profile id and the index of keys selected. The same can be used to reverse the data to obtain original one. The OPOBM model hikes data security performance in cloud.

Index Terms:
Cloud, SOA, Blockchain security, Data Encryption, OPOBM

Introduction:

The use of service orient architecture has been increased in recent times. The organizations provide number of services for their users which can be used to access the data. The cloud platform has been used to maintain the organizational data with least cost. However, the data maintenance in cloud faces variety of challenges in their security. There are number of threats can be named being faced by the cloud environment. The malicious user performs different illegal activities to degrade the service performance and to steal the cloud data. For example, the adversary would perform bruit force attack to learn the data from the cloud. Also, the services accessed by the user have been given with set of data which has been transferred through number of intermediate nodes in the internet. Presence of malicious node at any of the location would try to learn the data. To avoid this, there are number of access restriction and security checks prescribed earlier.

The trust based approaches restrict the data access through trust value which is computed based on the previous behavior in accessing the cloud data. Similarly, profile based approaches uses the profile as the key in identifying the trust of the user. Similarly, there are number of approaches can be named which challenge the threats. Still, the performance of the methods is highly compromising and does not suitable for modern day scenario.

The block chain technique is used in recent times which contain different blocks to carry the data which is cipher and hash code. The hash code is the key which represent the way how the data can be decrypted. Also, the block chain has a reference part to tell where to look the next block of data. By using block chain, the adversaries can be challenged efficiently. Still in this case, the data part can be decrypted by some adversaries and even they can try to learn what kind of encryption method is used. To handle this, different hash code methods are used earlier. In general, the hash code generation and decoding should be more dynamic and distinct for different profiles to challenge the adversary efficiently.

With all these consideration, an Optimal Profile Centric Blockchain Model (OPCBM) is presented in this paper. The method focused on using different set of encryption schemes and keys for distinct profiles. By choosing efficient key from the set by using radical profile id and by generating the hash code with the same, the performance of data security in cloud can be improved efficiently.

Related Works:

The methods of data security towards cloud environment are discussed in this section.

A blockchain based security model is given in [1], which applies logic of Burrows Abadi Needham (BAN) and ROR (Real or Random) model for data security. A two layer multidimensional security scheme is presented in [2], which uses block chain with low-latency, secure and reliable decision-making algorithm having powerful emergency handling capacity (LSRDM-EH) towards secure data transmission. A blockchain and fog-computing-enabled

security service architecture is presented inn [3], which uses equipment authentication and channel privacy protection to handle security issues.

Linear Elliptical Curve Digital Signature (LECDS) model is presented in [4], which applies blockchain with above mentioned algorithm to enforce data security with cloud. A public blockchain-envisioned secure communication framework for ITS (PBSCF-ITS) is presented in [5], which performs access control and key management for communication between vehicles. A blockchain based data security model is presented in [6], to support secure data communication in medical systems. The author analyzes different issues and challenges in the medical systems. A blockchain based security model is presented in [7], to support data security in Internet of Medical Things. The model enforce access control for health records according to the smart contracts used.

Merkle Hash Zero Correlation Distinguisher based blockchain security model is given in [8], to authenticate IoT devices in the cloud system. A deep learning model is presented in [9], which uses blockchain for secure data transmission in 5G networks. The model enforce data security in different layers of the environment. A software defined contract based block chain model is presented in [10], to support industrial IoT edge networks. The method authenticates the IoT devices with blockchain and smart contracts.

A two layer security model is presented in [11], which uses agile based model to secure relational data base through cloud services. An Byzantine fault tolerant scheme based environment monitoring system is presented in [12], which applies credit grouping supervision to reduce the computation and communication overhead. A blockchain based security and forensics management is presented in [13] for IoT, which analyze various issues in forensics management. A blockchain based security analysis technique is presented in [14], which classify the techniques into different categories like Burrows, Abadi, and Needham (BAN) logic, game theory, theory analysis, and AVISPA tool. A path compression based blockchain special key security (BSKM) technique is presented in [15], which integrates different elements of information security. A bloom filter based blockchain technique is presented in [16], which applies block chain security by performing access control with bloom filter.

All the above discussed approaches introduce poor performance in data security.

Optimal Profile Orient Blockchain Model (OPOBM):

The Optimized Profile Orient Blockchain Model (OPOBM) model receives the user request initially. From the user request, the set of data requested and need to be accessed are identified. The model classifies the users under various profiles and maintains set of key sets and scheme set for various profiles. According to the features identified, the method verifies the profile for the grant of access. Also, the method performs key selection and scheme from the profile with radical profile id. Using the radical profile id, the method selects the required encryption scheme and key to encrypt the data. Also, the method generates the hash code for distinct blocks based on the radical profile id and the index of keys selected. The same can be used to reverse the data to obtain original one. The detailed working is sketched in this section.

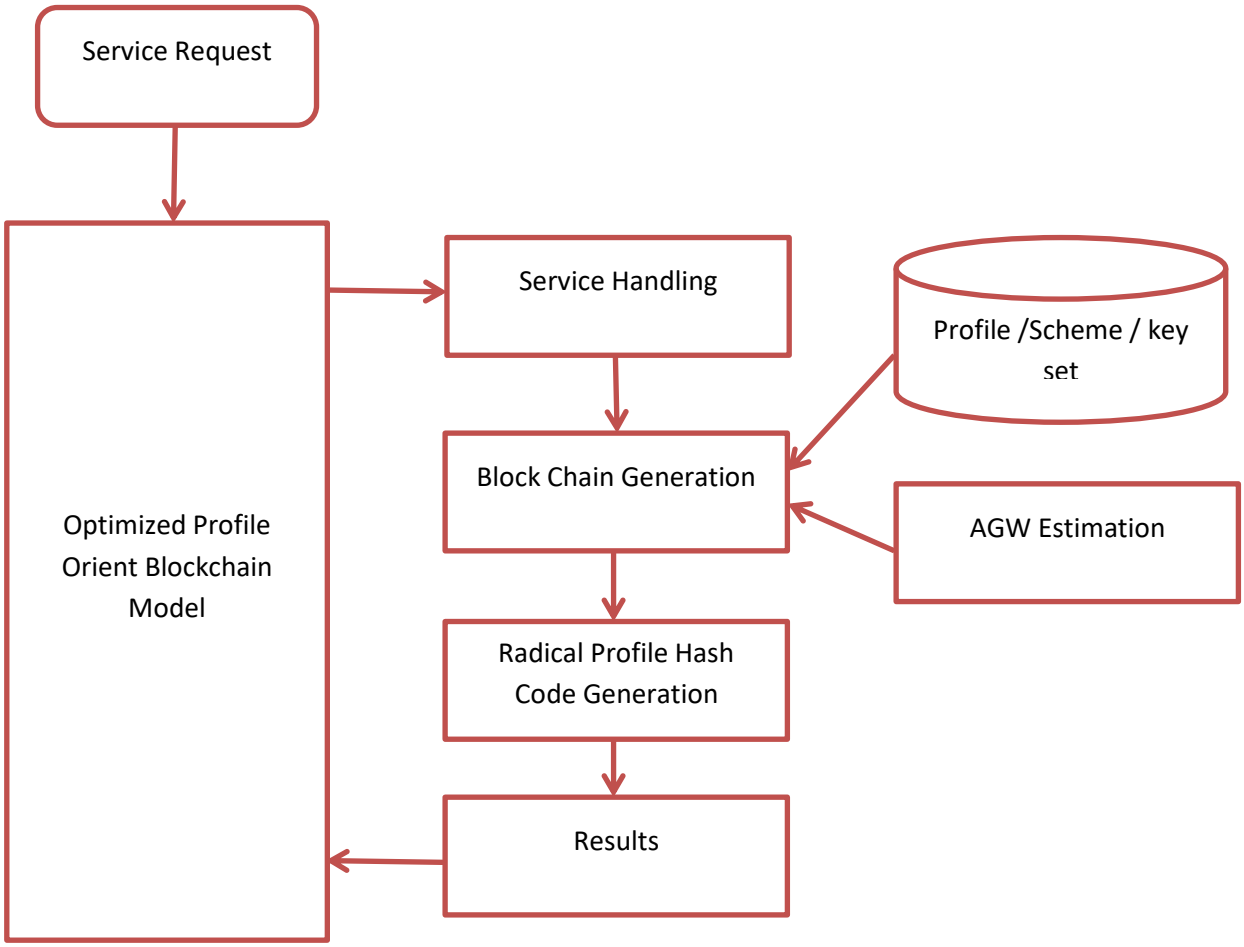

Figure 1: Architecture of Proposed OPOBM Model

The working sequence of OPOBM model is displayed in Figure 1, where the complete working of each function is detailed here.

Service Handling:

The service handling function is responsible for receiving the service request from the user. From the request, the method should identify what service is requested and what are the features the service is accessing. Using these details, the method estimates the Access grant weight (AGW) for the user according to the profile given. If the value of AGW is higher than the acceptable value, then the user is allowed to access the data, otherwise the user will be denied from accessing the service data. Further, the method performs block chain generation and Radical Profile Hash code generation to complete the process. Obtained blockchain has been returned as result to the user.

Algorithm:

Given: Profile data Pd, Service Request Sr

Obtain: Blockchain B

Start

Read Pd and Sr.

Service s = $Service\_Id \in Sr$

Feature list Fl = $\sum_{i=1}^{Size(Sp)} Features \rightarrow Sp(i) \; where \; Sp(i).id == S.id$

Compute AGW = $\frac{\sum_{i=1}^{size(Fl)} \sum_{j=1}^{Size(Pd)} Count(Pd(j)==Fl(i) \;\&\&\; Pd(j).user==sr.user)}{size(Fl)}$

If AGW>Th then

If request.type is access then

Blockchain B = Perform Blockchain Generation

Perform Radical Profile Hash Generation.

Send result to the user

Else

For each feature f

Perform verification.

End

Update data to cloud.

Else

Deny access.

End

Stop

The working of service handling function is presented in above pseudo code which restricts the user access according to the AGW value measured and generates the block chain. Also the method applies radical profile hash generation to complete the process.

Blockchain Generation:

The proposed method generates a block chain as per the profile of user. From the profile and the set of features being accessed, the method generates the block chain with k number of blocks. Each feature has been encoded in the distinct block, where the method encrypt the data with specific distinct encryption scheme and key dictated for profile. The method maintains set of schemes and key set to support the encryption process. To identify the scheme for each feature, the method applies radical profile id as the key to be used toward the selection of key and scheme. For example, if the radical profile id is “US001HS” which denotes “United Service 001 House Surgeon”. From the radical id, the method counts the numeric value of the all the digits. The digits are summed to get a whole number. If the whole number is “21+19+0+0+1+8+21”=70, then the method get the modulus value of 26 which denotes the total

alphabets. This operation yields the value of 18, which denotes the index of scheme and key to be selected. Concern scheme and key selected has been used to encrypt the data. Each block has been iterated with the same process to generate the block chain.

Algorithm:

Given: Profile Data Pd, Service S

Obtain: Blockchain B

Start

Read Pd and S.

Radical id Rid = $Pd(i).Rid? \underset{i=1}{\overset{Size(Pd)}{} } Pd(i).Uid == S.uid$

Scheme set Ss = $Pd(i).schemeset? \underset{i=1}{\overset{Size(Pd)}{} } Pd(i).Rid == Rid$

Key set Ks = $Pd(i).keyset? \underset{i=1}{\overset{Size(Pd)}{} } Pd(i).Rid == Rid$

Feature set Fl = $Pd(i).Features? \underset{i=1}{\overset{Size(Fl)}{} } Pd(i).s == s.sid$

Generate blockchain B = $Generate\ Block\ and\ add\ to\ chain \underset{i=1}{\overset{Size(Rid)}{}}$

Compute radical index Ri = $sum\left(Numeric\left(Rid(i)\right)\right) Mod\ 26 \underset{i=1}{}$

For each block b

Scheme index Si = Rand(ss,Ri)

Key index ki = Rand(ks,Ri)

Cipher text CT = Encrypt(b.data,ss(si),ks(ki))

Add CT to block b.

Perform Generate radical hash code generation.

End

Stop

The blockchain generation scheme uses radical index from the radical id to perform data encryption.

Radical Profile Hash Code Generation:

The radical profile hash code generation algorithm generates the hash code according to the given radical index with the index of scheme index and key index. The radical index, scheme index and key index are separated with a hash symbol. Generated has code has been added to the hashing part of the block given.

Algorithm:
Given: Block Chain B, Block index bi, radical index Ri, Scheme index Si, key index ki
Obtain: Block chain B
Start
Read B, bi, ri, si, ki
Hash code Hc = Ri+"#"+Si+"#"+ki
B(Bi).Hash code = Hc
Stop

The above discussed algorithm generates the hash code according to the radical index, key index and scheme index provided.

Results and Discussion:

The proposed optimized profile orient blockchain model is simulated using Advanced java and evaluated for its performance in different parameters.

Parameter	Value
Tool	Advanced Java
Number of users	200
Number of features	50
Number of services	100

Table 1: Evaluation Details

The environment details used for performance evaluation is given in Table 1.

Security Performance vs Number of Services			
	25 Services	50 services	100 Services
BAN	69	73	77
LECDS	73	77	82
LSRDM-EH	77	81	87
OPOBM	84	89	96

Table2: Analysis on security performance

The performance in security is measured for various methods and presented in Table 2, where the proposed OPOBM model produces higher security performance than other methods.

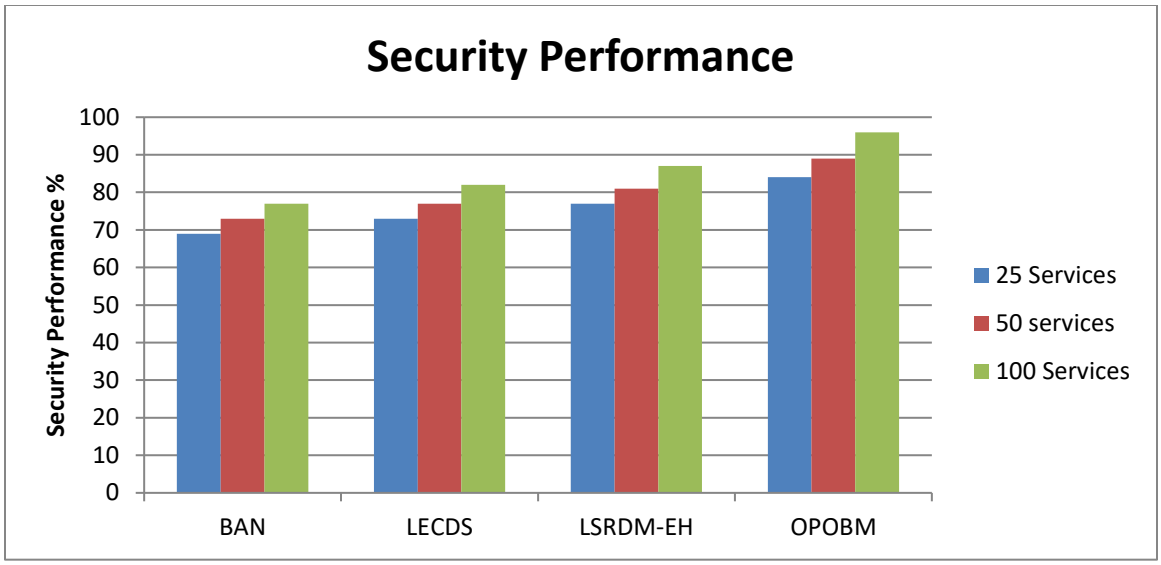

Figure 2: Analysis on security performance

The performance security is measured and compared in Figure 2, and OPOBM has produced higher security performance than other methods.

Throughput Performance vs Number of Services			
	25 Services	50 services	100 Services
BAN	68	72	76
LECDS	72	76	81
LSRDM-EH	76	82	84
OPOBM	84	88	97

Table3 Analysis on throughput performance

The performance in throughput is measured for various methods and presented in Table 3, where the proposed OPOBM model produces higher throughput performance than other methods.

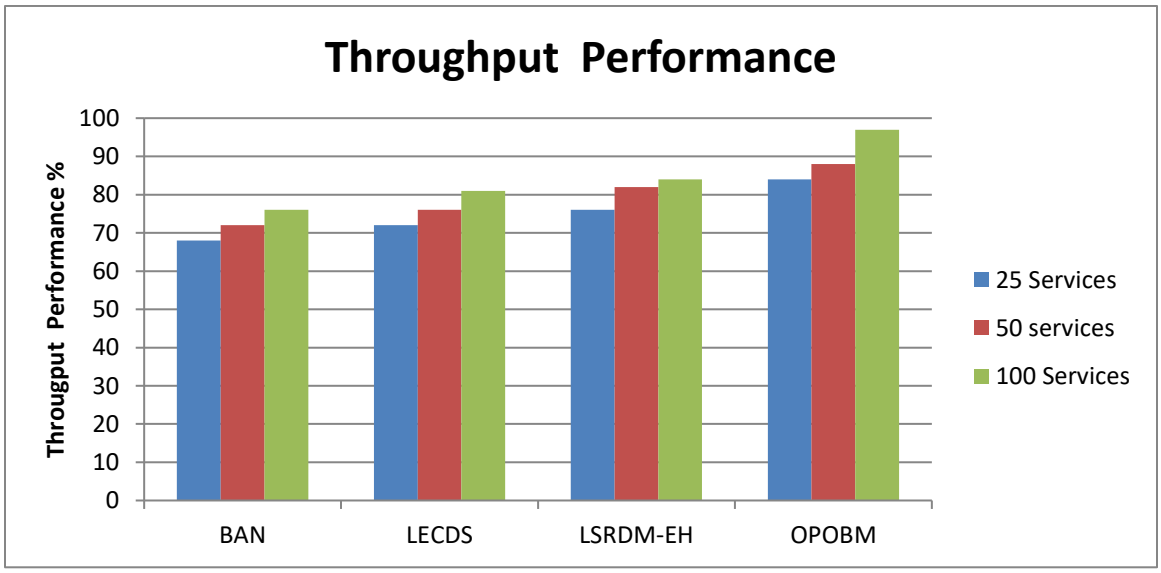

Figure 2: Analysis on security performance

The performance security is measured and compared in Figure 2, where the proposed OPOBM has produced higher security performance than other methods.

Conclusion:

This paper presented a Optimized Profile Orient Blockchain Model (OPOBM) model towards data security in cloud. The method receives the user request initially and identifies the set of data need to be accessed. According to the features identified, the method verifies the profile for the grant of access. Also, the method performs key selection and scheme from the profile with radical profile id. Using the radical profile id, the method selects the required encryption scheme and key to encrypt the data. Also, the method generates the hash code for distinct blocks based on the radical profile id and the index of keys selected. The same can be used to reverse the data to obtain original one. The method introduces higher performance in data security with higher throughput.

References:

1. G. Thakur, P. Kumar, Deepika, S. Jangirala, A. K. Das and Y. Park, "An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment," in IEEE Access, Volume. 11, pp. 26877-26892, 2023.
2. J. Ren, J. Li, H. Liu and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," IEEE (TS&T), Volume. 27, Number 4, pp. 760-776, 2022.
3. T. Hewa, A. Braeken, M. Liyanage and M. Ylianttila, "Fog Computing and Blockchain-Based Security Service Architecture for 5G Industrial IoT-Enabled Cloud Manufacturing," IEEE (TII), Volume. 18, Number 10, pp. 7174-7185, 2022.
4. B. Sowmiya, E. Poovammal, K. Ramana, S. Singh and B. Yoon, "Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced Security on Cloud Server," in IEEE Access, Volume. 9, pp. 138245-138253, 2021,
5. M. Wazid, B. Bera, A. K. Das, S. P. Mohanty and M. Jo, "Fortifying Smart Transportation Security Through Public Blockchain," IEEE (ITJ), Volume. 9, Number 17, pp. 16532-16545, 2022.
6. Q. Liu, Y. Liu, M. Luo, D. He, H. Wang and K. -K. R. Choo, "The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities," IEEE (SJ), Volume. 16, Number 4, pp. 5741-5752, 2022.
7. B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control," IEEE (ITJ), Volume. 8, Number 14, pp. 11717-11731, 2021.
8. R. Patan, R. Manikandan, R. Parameshwaran, S. Perumal, M. Daneshmand and A. H. Gandomi, "Blockchain Security Using Merkle Hash Zero Correlation Distinguisher for the IoT in Smart Cities," IEEE (ITJ), Volume. 9, Number 19, pp. 19296-19306, 2022.
9. S. Rathore, J. H. Park and H. Chang, "Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT," in IEEE Access, Volume. 9, pp. 90075-90083, 2021.

10. P. Krishnan, K. Jain, K. Achuthan and R. Buyya, "Software-Defined Security-by-Contract for Blockchain-Enabled MUD-Aware Industrial IoT Edge Networks," IEEE (TII), Volume. 18, Number 10, pp. 7068-7076, 2022.
11. R. Awadallah and A. Samsudin, "Using Blockchain in Cloud Computing to Enhance Relational Database Security," in IEEE Access, Volume. 9, pp. 137353-137366, 2021.
12. M. Zhao, W. Liu and K. He, "Research on Data Security Model of Environmental Monitoring Based on Blockchain," in IEEE Access, Volume. 10, pp. 120168-120180, 2022.
13. Z. Liao, X. Pang, J. Zhang, B. Xiong and J. Wang, "Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey," IEEE (TN&SM), Volume. 19, Number 2, pp. 1159-1175, 2022.
14. M. A. Ferrag and L. Shu, "The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial,"IEEE (ITJ), Volume. 8, Number. 24, pp. 17236-17260, 2021.
15. C. Bakir, "New Blockchain Based Special Keys Security Model With Path Compression Algorithm for Big Data," in IEEE Access, Volume. 10, pp. 94738-94753, 2022.
16. R. Li, Y. Qin, C. Wang, M. Li and X. Chu, "A Blockchain-Enabled Framework for Enhancing Scalability and Security in IIoT," IEEE (TII), Volume 19, Number 6, pp. 7389-7400, 2023.