Empirical Analysis of Block chain and Machine Learning inspired Cloud Security Architectures

Anand Deepak George Donald
Research Scholar, Department of Computer Science Engineering, LNCT University, Bhopal, India.
Email id: anand1donald1980@gmail.com

Article Received: 10 July 2021 *Article Accepted: 5 Oct 2021* *Article Published: 30 Nov 2021*

Citation
Anand Deepak George Donald. (2021). Empirical Analysis of Block chain and Machine Learning inspired Cloud Security Architectures, *Journal of Next Generation Technology*, 1(2), 20-28.

Abstract

A Cloud deployment consists of compute and storage components. Both these components are responsible for interacting with user data, which is under constant threats from spies, malicious bots, attackers, etc. Most of this data on public clouds consists of photos, videos, and non-confidential data, which has low security requirement. But some of this data might consist of Bank statements, permanent account number (PAN) information, address information, passport data, etc. Moreover, almost all the data on private cloud requires high security, because this data is highly confidential and must not be leaked. In order to provide security to both the data and the compute components, it is necessary to deploy cryptographic and hashing algorithms. These algorithms provide high level of security for centralized data storage, but the security performance reduces when data is stored on multiple cloud servers present at different locations. In order to strengthen the security performance for this kind of storage, different machine learning and blockchain based systems are proposed by researchers over the years. Some of these algorithms are suited for small scale to medium scale deployments, while others are applicable only for large-scale cloud systems. Also, deploy-ability of these algorithms depends heavily on the computational and quality of service (QoS) performance of these algorithm. Therefore, it is difficult for network designers and researchers to select the best algorithms suited for their specific applications. In order to do this, network designers and researchers have to either indulge into the literature of these algorithms, or deploy these algorithms on a sandbox for testing their performance on a small set of data & then estimate their performance for large data. Performing this task is very cumbersome, and limits the ability of network designers to evaluate best algorithms for their given deployment. In order to facilitate optimum algorithm selection this text reviews some of the recent security architectures used for securing cloud deployments at both server level and client level. This text also compares these algorithms based on the scale of cloud deployment, on various factors such as security level, speed of operation, etc. to assist cloud deployers for selecting algorithm(s) which are best suited for their given application.

Keywords: Cloud, security, machine learning, blockchain, QoS.

I. Introduction

Cloud deployments are under constant need upgradation due to various performance and security patches. These upgradations and new deployments interface with the original deployment to extend cloud's functionality and make it more useable. Most of the times this integration introduces certain security holes into the system, due to which the overall data confidentiality is affected. Each cloud deployment works with at-least 4 layers of deployment, which can be described as follows,

Cloud user layer, wherein cloud users are present. These users request access to use cloud services and store/retrieve data.

Cloud automation layer, which analyses user requests, plans the execution, executes these requests and finally monitor the responses of these requests. This layer is largely responsible for all kind of QoS and security settings in the cloud deployment.

Security layer is followed by this layer, wherein different kinds of security algorithms like encryption, hashing, key-exchange, etc. are applied. This layer introduces different security parameters to the system, and makes the system accessible to only restricted set of users.

Secure cloud storage layer, wherein all data transacted in the network is stored. This data is read and written only after certain security constraints are met in the network.

A blockchain powered network consisting of these layers can be observed in figure 1, wherein the security layer is replaced with Blockchain management layer, and secure storage layer is replaced with blockchain cloud storage layer.

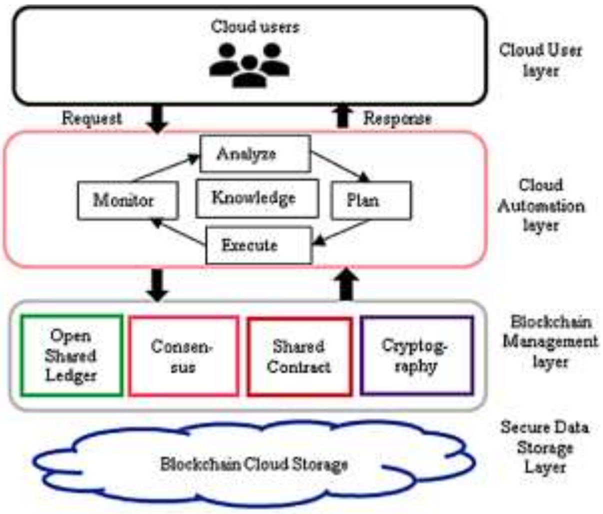

Fig.1. An example secure cloud deployment using blockchain

Apart from blockchain, other security paradigms are also widely used by researchers. The next section describes different security structures proposed by researchers in the past couple of years. This is followed by the comparative analysis of these algorithms via delay & security parameters. Finally, this text concludes with some interesting observations about these algorithms and suggests methods to improve them.

II. Literature Review

Enabling security for cloud deployments have always been a challenging task. Various algorithms have been proposed for managing security at different cloud levels. These levels include but are not limited to, client-side security, communication security, computational security, data storage security, etc. From the research showcased in [1], it can be observed that blockchain and its variants have been most successful in improving security for cloud deployments. This security is measured in terms of Confidentiality, data integrity, data & user anonymity, privacy protection, residual information protection & attack detection. The work also suggests that machine learning protocols are one of the most commonly used security protocols for cloud networks. Using this research, it can be observed that most of the recent security solutions are based on blockchain and its machine learning-based variants. One such variant can be observed in [2], wherein machine learning is used for identification of analytical parameters to be used for the given cloud application. A use-case of Industrial Internet of Things (IIOT) is considered for reference. This work suggests that parameters like throughput, delay & packet loss ratio must be analysed on the basis of interoperability, convergence and reliability to design a highly secure QoS aware blockchain solution. An analytic hierarchy process (AHP) is described which identifies best case parameters that can be used for optimum security in the proof-of-work based blockchain deployment. Moderate level of security with moderate throughput performance can be obtained with the help of AHP based cloud deployments. This work can be extended via [3] to add the concept of privacy improvement. The work in [3] suggests use of hybrid encryption for storing data. The hybrid encryption is basically a set of encryption algorithms which are connected in a manner, such that overall security of the system improves when compared with individual encryption performance. This algorithm shown in figure 2, results into a highly secure blockchain system, with limited focus on cloud QoS, and thus cannot be applied to large scale or IoT enabled cloud deployments.

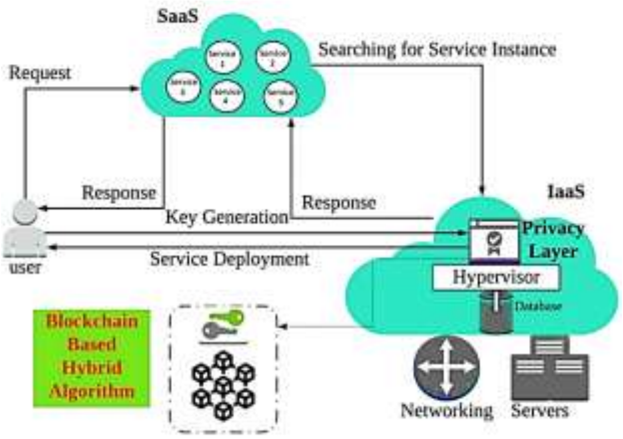

Fig. 2. Blockchain deployment with hybrid encryption for improved security [3]

This might not affect many small to medium scale deployments, but in todays connected world, where most of the IoT applications are dependent on cloud [4], this system might not be real-time deployable. To overcome this drawback, the work in [5] is proposed. This work uses least significant bit (LSB) based encryption technique along with mixed linear and nonlinear spatiotemporal chaotic systems (MLNCML) for improved security performance in IoT networks. Due to the use of LSB technique, a fine-grained control over the access of IoT devices is obtained. This control is backed up by the MLNCML algorithm to provide high security via randomized encryption keys. The system is tested on image data, but can be equally applied to text, audio and video datasets. Due to the use of MLNCML algorithm, the system is highly secure, and has moderate QoS which is passable for any IoT-based cloud deployment. The system's security hasn't been tested against different kinds of attacks. It is recommended that researchers perform this security analysis before deploying the proposed system for real-time use-cases. Attack analysis can be observed from [6], wherein different kinds of routing attacks are detected in Low Power and Lossy Cloud IoT Networks. Blockchain is used to strengthen its security with the help of smart contracts. These contracts are useful in raising real-time alerts in case unwanted or malicious packets are communicated in the network. Due to use of smart contracts, the energy efficiency of this system is high, but the delay performance is low, which reduces speed of operation, thereby requiring high speed networks for real-time usage. It has an accuracy of 91% for routing attacks detection, but this accuracy can be improved further using machine learning models for packet analysis. The system can be further tested on other cloud attacks like Node Tampering, RF Interference on RFIDs, Node Jamming Adversaries, Malicious Node

Injection, Insecure Initialization, Sleep Deprivation Attack, Sybil and Spoofing Attacks and Malicious Code Injection as mentioned in [7].

Cloud-based supply chain systems (SCM) can also be secured with the help of blockchain-based solutions. The work in [8] proposes the use of ERC20 interface for a permissioned blockchain to improve its security. ERC20 interface is based on the Ethereum blockchain, and thus uses smart-contracts with proof-of-stake for low power and high throughput security applications. Architecture for this system can be observed from figure 3, wherein each of the cloud-based supply chain management entities are showcased. These entities are linked with each other using smart-contracts. Each smart contract stores the following information,

- The hash value of previous block
- A nonce number to generate unique hashes
- Hash of the current block, and the current block number
- The transaction index, or primary key for this block
- Some input data about the transaction which can include,
- Buyer identification
- Seller identification
- Goods identification
- Other transaction information
- Price to perform one transaction on this block, a.k.a. gas value

Other cloud applications can also use blockchain technologies for improving their security. A list of these applications & suitable blockchains can be observed from [9]. Blockchain variants like Bitcoin, Dodgecoin, Monero, Litecoin, hyper-ledger fabrics, multi-chains, etc. are described in this paper. They suggest that blockchain can be used for different cloud applications including but not limited to, agriculture, construction, Education, Government, Healthcare, Supply chain, Voting, etc. The main issue with these blockchain applications is the inability to perform data search on secure blocks. The work in [10] overcomes this drawback with the use of Interplanetary File System (IPFS) and double-layer blockchain. Due to the use of double blockchain, the system stores an indexed copy of the chain with itself. This indexed copy is not-encrypted and is stored internally with the server itself. While performing search, this internal copy (consortium chain) is scanned, and indexes are found. The indexes are then used on the main blockchain to return the results. An architecture diagram for this search process can be observed in figure 4, wherein the consortium blockchain searching with public chain retrieval is shown.

This process reduces the delay of operation, but increases the storage requirements on the cloud. The system can be used for small to medium tier applications, but is not applicable to large scale deployments due to the use of the consortium chain. This drawback can be removed using local distributed side-chains. Such side-chains are mentioned in [11] using multi-stake holder concept. Application of such side chain-based consortium networks can be further extended for financial services. The work in [12] suggests the use of locally stored indexed side-chains for high speed and low-energy secure transactions. These networks provide high level of security but have exponential storage requirements, and thus must only be used for private search operations, which is a drawback of this architecture. This drawback can be removed by deploying the consortium blockchains as service over cloud. Such an architecture can be observed in [13], wherein bartering functionalities for the H2020 symbIoTe framework are secured. This system uses proof of authority (PoA) consensus for improving security along with reduced delay and memory requirements for small to large scale applications. This scheme has good security and QoS performance, but its consistency can be improved by using auditing mechanisms. Auditing mechanisms will test the blockchain's performance and audit it for any internal issues. These audits allow blockchain system designers to eliminate the detected issues, and improve the overall security & QoS consistency of the network. Such a public auditing scheme without trusted auditors can be observed in [14]. Due to the non-dependency on trusted auditors, this scheme has high security and thus is resilient to malicious trusted auditor attacks. These attacks are removed by replacing the auditors with distributed miners. These distributed miners are located at different physical nodes, and thereby do not interact with one another to perform a cumulative attack. This system has high security, but due to the use of miner-based trust mechanisms the QoS is reduced. The system can be replaced with the improved blockchain-based authentication protocol (IBCbAP) as mentioned in [15], which ensures high QoS and low attack probability with high consistency, but is only applicable for IoT-enabled cloud systems. The trust value can also be improved using the controllable blockchain data management (CDBM) mentioned in [16]. This algorithm reduces the dependency of blockchain deployments on auditors by adding a local trust-authority with set of overlapping users. This trust authority validates the users, and gives this feedback to the central controller. The controller is able to validate users based on overlapping responses from these trust authorities to decide which authorities are functioning and which ones are compromised. This feature also reduces the need of miners for auditing the blockchain, and improves the overall QoS, security and consistency performance.

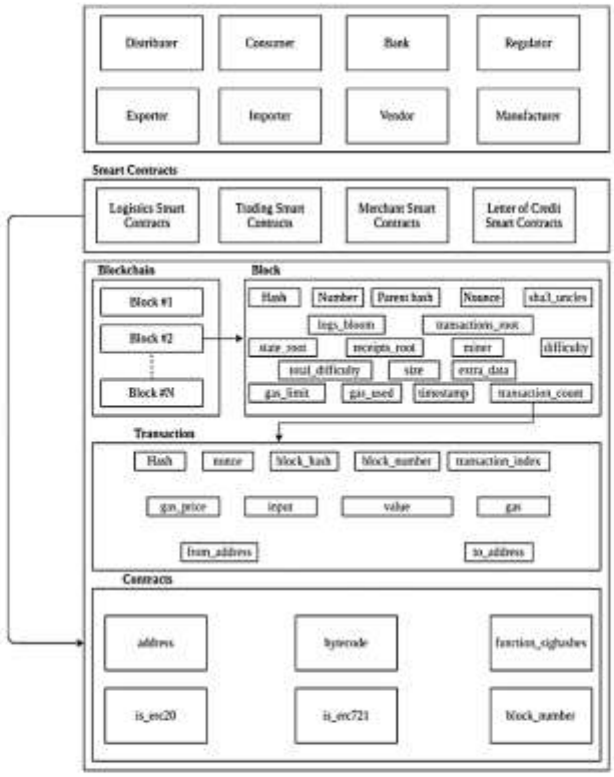

Fig. 3. Ethereum based cloud security framework for SCM [8]

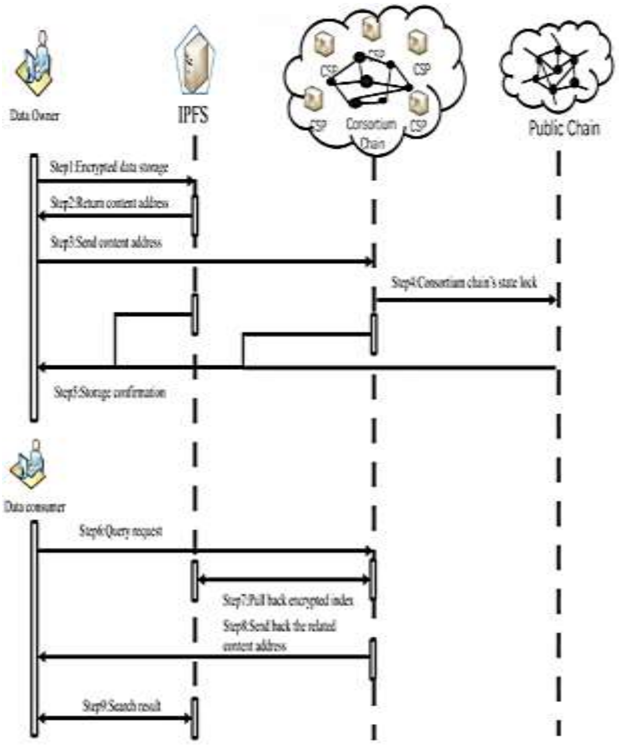
Data Owner
IPFS
CSP
CSP
CSP
CSP
CSP
Consortium Chain
Public Chain
Step1:Encrypted data storage
Step2:Return content address
Step3:Send content address
Step4:Consortium chain's state lock
Step5:Storage confirmation
Data consumer
Step6:Query request
Step7:Pull back encrypted index
Step8:Send back the related content address
Step9:Search result

Fig. 4. Double indexed blockchain for searching in encrypted domain [10]

Cloud-based blockchains can also be applied to eVoting systems. One such implementation of blockchain for eVoting can be observed in [17]. The system uses Ethereum based smart contracts for voting, user verification and vote counting. While Ethereum is a defacto-standard for most blockchain implementations, it requires complex computations for effective deployment and use, thereby reducing its delay performance. The work in [18] proposes the use of a light-weighted authentication mechanism that can be used for user verification purposes for improved delay performance. This light-weighted protocol uses device identification information to authenticate the devices for better security performance against authentication attacks. A survey of such attacks and their defence mechanisms for cloud deployed blockchains can be observed from [19]. From this review it can be confirmed that blockchain is suitable for any scale of cloud deployment, and has better security, QoS and scalability features. An application of blockchain applied to cloud-based medical health-care is observed in [20], wherein a proof-of-work (PoW) based blockchain is used. Another application of blockchain to cloud-based automotive security can be observed from [21], wherein both PoW and proof-of-stake (PoS) are used to provide security to the chain.

All these blockchain based deployments have an inherent drawback of reduced QoS during deployment. Some of the techniques claim to improve the QoS, but are not able to do so. This is because the complexity of chain creation increases exponentially as the blockchain length increases.

III. Comparative Analysis

In order to compare performance of the reviewed algorithms, this section uses the following entities of comparison,

- Delay (D) needed to provide security, which indicates latency of system after the said security algorithm is applied to it.
- Security level (SL), which indicates the attack detection performance of the system.
- Application area (AA), this suggests the applications for which the given algorithm is applicable
- Energy (E) requirement, which is an indicative of the cloud-power consumption

Table. 1. Comparative analysis of the reviewed algorithms

Method	D	SL	E	AA
AHP with PoW [2]	H	H	M	IIoT clouds
Hybrid encryption [3]	H	H	H	General cloud systems
LSB with MLNCML [5]	M	H	M	IoT clouds
Smart contracts [6]	H	H	M	General cloud systems
ERC20 for permissioned blockchain with PoS [8]	H	H	L	SCM
IPFS with Double layer blockchain [10]	M	H	H	General cloud systems
Multi-holder stake [11]	M	M	M	General cloud systems
Local stored consortium chains [12]	L	M	M	General cloud systems
Blockchain as a service with PoA [13]	M	H	M	General cloud systems
Distributed miners for trust establishment [14]	H	H	M	General cloud systems
IBCbAP [15]	M	H	L	General cloud systems
CDBM [16]	H	H	M	General cloud systems
Smart contracts [17]	H	H	H	eVoting systems
Light weighted authentication [18]	M	H	M	General cloud systems
PoW [20, 21]	H	M	M	Health care and auto industry
Anomaly detection, clustering and classification [22]	M	M	M	General cloud systems

CNNs [23]	M	H	M	General cloud systems
Cognitive CAPTCHAs [24]	H	H	M	General cloud systems
RNN [25]	H	H	M	Cloud cyber security
ResNet and VGGNet [26]	H	H	M	Edge cloud devices
GAN [29, 30]	H	H	H	General cloud systems
Big data analysis [31, 32]	M	H	M	General cloud systems

From the review it is inherent that multi-holder stake algorithms based on consortium based blockchains & PoA-based blockchains outperform other block chains in terms of security level, energy utilization and delay performance. These blockchains can be combined with machine learning algorithms [2] like CNNs, RNNs and GANs to further improve their security and reliability.

IV. Conclusion and future scope

Blockchains have become a very valuable tool for securing cloud deployments. Some blockchain-based networks like the ones mentioned in [2] use machine learning for improved QoS and security performance. Ethereum-based PoW, PoS and PoA blockchains outperform other blockchain architectures, but they can be improved using hybrid encryption and light-weight authentication mechanisms. Moreover, the blockchain perfrmance can be improved by integration of machine learning models like CNNs and RNNs. These models are not yet integrated with blockchains for providing cloud security, and thus can be an interesting avenue of work for cloud researchers.

References

[1]. Mayuranathan, M., Murugan, M. &Dhanakoti, V. Enhanced security in cloud applications using emerging blockchain security algorithm. *J Ambient Intell Human Comput* 12, 6933–6945 (2021). https://doi.org/10.1007/s12652-020-02339-7

[2]. Sodhro, A.H., Pirbhulal, S., Muzammal, M. *et al.* Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications. *J Grid Computing* 18, 615–628 (2020). https://doi.org/10.1007/s10723-020-09527-x

[3]. Darwish, M.A., Yafi, E., Al Ghamdi, M.A. *et al.* Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm. *Arab J Sci Eng* 45, 3369–3378 (2020). https://doi.org/10.1007/s13369-020-04394-w

[4]. Memon, R.A., Li, J.P., Ahmed, J. *et al.* Cloud-based vs. blockchain-based IoT: a comparative survey and way forward. *Front Inform Technol Electron Eng* 21, 563–586 (2020). https://doi.org/10.1631/FITEE.1800343

[5]. Liu, Y., Zhang, J. & Zhan, J. Privacy protection for fog computing and the internet of things data based on blockchain. *Cluster Comput* 24, 1331–1345 (2021). https://doi.org/10.1007/s10586-020-03190-3

[6]. Sahay, R., Geethakumari, G. & Mitra, B. A novel blockchain based framework to secure IoT-LLNs against routing attacks. *Computing* 102, 2445–2470 (2020). https://doi.org/10.1007/s00607-020-00823-8

[7]. Rudra, B. (2020). IMPACT OF BLOCKCHAIN FOR INTERNET OF THINGS SECURITY. In Cryptocurrencies and Blockchain Technology Applications (eds G. Shrivastava, D.-N. Le and K. Sharma). https://doi.org/10.1002/9781119621201.ch6

[8]. Kumar, A, Abhishek, K, Nerurkar, P, Ghalib, MR, Shankar, A, Cheng, X. Secure smart contracts for cloud-based manufacturing using Ethereum blockchain. *Trans Emerging Tel Tech*. 2020;e4129. https://doi.org/10.1002/ett.4129

[9]. Akram, SV, Malik, PK, Singh, R, Anita, G, Tanwar, S. Adoption of blockchain technology in various realms: Opportunities and challenges. *Security and Privacy*. 2020; 3:e109. https://doi.org/10.1002/spy2.109

[10].Fu, S, Zhang, C, Ao, W. Searchable encryption scheme for multiple cloud storage using double-layer blockchain. *Concurrency ComputatPractExper*. 2020;e5860. https://doi.org/10.1002/cpe.5860

[11].C. V. N. U. B. Murthy, M. L. Shri, S. Kadry and S. Lim, "Blockchain Based Cloud Computing: Architecture and Research Challenges," in IEEE Access, vol. 8, pp. 205190-205205, 2020, doi: 10.1109/ACCESS.2020.3036812.

[12].Nathan, J, Jacobs, B. Blockchain consortium networks: Adding security and trust in financial services. *J Corp Acct Fin*. 2020; 31: 29– 33. https://doi.org/10.1002/jcaf.22428

[13].Tedeschi, P, Piro, G, Murillo, JAS, et al. Blockchain as a service: Securing bartering functionalities in the H2020 symbIoTe framework. *Internet Technology Letters* 2019; 2:e72. https://doi.org/10.1002/itl2.72

[14].Song Li, Jian Liu, Guannan Yang, Jinguang Han, "A Blockchain-Based Public Auditing Scheme for Cloud Storage Environment without Trusted Auditors", *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8841711, 13 pages, 2020. https://doi.org/10.1155/2020/8841711

[15].Mostafa Yavari, Masoumeh Safkhani, Saru Kumari, Sachin Kumar, Chien-Ming Chen, "An Improved Blockchain-Based Authentication Protocol for IoT Network Management", *Security and Communication Networks*, vol. 2020, Article ID 8836214, 16 pages, 2020. https://doi.org/10.1155/2020/8836214

[16].Zhu, Liehuang& Wu, Yulu& Gai, Keke & Choo, Kim-Kwang Raymond. (2018). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems. 91. 10.1016/j.future.2018.09.019.

[17].Krishnamurthy, R., Rathee, G. &Jaglan, N. An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices. *Wireless Netw* 26, 2391–2402 (2020). https://doi.org/10.1007/s11276-019-02112-5

[18].Khalid, U., Asim, M., Baker, T. *et al.* A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Comput* 23, 2067–2087 (2020). https://doi.org/10.1007/s10586-020-03058-6

[19].Blockchain for Distributed Systems Security, https://www.wiley.com/en-in/Blockchain+for+Distributed+Systems+Security-p-9781119519607

[20].Saha, A, Amin, R, Kunal, S, Vollala, S, Dwivedi, SK. Review on “Blockchain technology based medical healthcare system with privacy issues”. *Security and Privacy*. 2019; 2:e83. https://doi.org/10.1002/spy2.83

[21].A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," in IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125, Dec. 2017, doi: 10.1109/MCOM.2017.1700879.

[22].Rajkumar Buyya; Satish Narayana Srirama, "Using Machine Learning for Protecting the Security and Privacy of Internet of Things (IoT) Systems," in Fog and Edge Computing: Principles and Paradigms , Wiley, 2019, pp.223-257, doi: 10.1002/9781119525080.ch10.

[23].Zeadally, S, Tsikerdekis, M. Securing Internet of Things (IoT) with machine learning. *Int J Commun Syst*. 2020; 33:e4169. https://doi.org/10.1002/dac.4169

[24].Ogiela, U. Cognitive cryptography for data security in cloud computing. *Concurrency ComputatPractExper*. 2020; 32:e5557. https://doi.org/10.1002/cpe.5557

[25].Sakthivel, RK, Nagasubramanian, G, Al-Turjman, F, Sankayya, M. Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. *Trans Emerging Tel Tech*. 2020;e3947. https://doi.org/10.1002/ett.3947

[26].Z. Tian, C. Luo, J. Qiu, X. Du and M. Guizani, "A Distributed Deep Learning System for Web Attack Detection on Edge Devices," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1963-1971, March 2020, doi: 10.1109/TII.2019.2938778.

[27].Muhammad Imran Tariq, Nisar Ahmed Memon, Shakeel Ahmed, Shahzadi Tayyaba, Muhammad Tahir Mushtaq, Natash Ali Mian, Muhammad Imran, Muhammad W. Ashraf, "A Review of Deep Learning Security and Privacy Defensive Techniques", *Mobile Information Systems*, vol. 2020, Article ID 6535834, 18 pages, 2020. https://doi.org/10.1155/2020/6535834

[28].Butt UA, Mehmood M, Shah SBH, Amin R, Shaukat MW, Raza SM, Suh DY, Piran MJ. A Review of Machine Learning Algorithms for Cloud Computing Security. *Electronics*. 2020; 9(9):1379. https://doi.org/10.3390/electronics9091379

[29].Vemulapalli C., Madria S.K., Linderman M. (2020) Security Frameworks in Mobile Cloud Computing. In: Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security. Springer, Cham. https://doi.org/10.1007/978-3-030-22277-2_1

[30].Panda D.R., Behera S.K., Jena D. (2021) A Survey on Cloud Computing Security Issues, Attacks and Countermeasures. In: Patnaik S., Yang XS., Sethi I. (eds) Advances in Machine Learning and Computational Intelligence. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-15-5243-4_47

[31].Stergiou C.L., Plageras A.P., Psannis K.E., Gupta B.B. (2020) Secure Machine Learning Scenario from Big Data in Cloud Computing via Internet of Things Network. In: Gupta B., Perez G., Agrawal D., Gupta D. (eds) Handbook of Computer Networks and Cyber Security. Springer, Cham. https://doi.org/10.1007/978-3-030-22277-2_21

[32].Mishra, Bharati & Jena, Debasish. (2021). Mitigating Cloud Computing Cybersecurity Risks Using Machine Learning Techniques. 10.1007/978-981-15-5243-4_48.