Journal of Engineering and Applied Sciences 14 (17): 6525-6532, 2019
ISSN: 1816-949X

A Blockchain-Based Hybrid Algorithm for Data Privacy at Cloud Storage

[1]Marwan Adnan Darwish, [1]Eiad Yafi, [2]Habib Ur Rehman and [3]Mohammad A. Al Ghamdi
[1]Malaysian Institute of Information Technology, University Kuala Lumpur,
1016 Jalan Sultan Ismail, 50200 Kuala Lumpur, Malaysia
[2]DXN Technologies New Delhi, Delhi, India
[3]Computing and Information Systems College, Umm Al-Qura University, Mecca, KSA
Marwan.khabbaz1@gmail.com

Abstract: Information security is critical to the development of modern internet technologies. The features of blockchain technology such as distributed approaches, decentralized mechanism, password mechanism and scripted mechanism present a completely new perspective for the development of internet information security technology. Cloud storage, like any other untrusted environment, requires the ability to secure shared information and ensure data privacy and reliability. The traditional solutions such as encryption have not been successful in preventing software bugs and misconfiguration issues. In this study, we present the framework of a blockchain-based public key encryption algorithm to ensure the privacy of user's data at the infrastructure layer of the cloud platform. This technique encrypts the data to cipher form and then incorporate the Cipher-texts into hash codes as a digital signature on blockchain ledger to guarantee data integrity. The results depict an outbreak in the data security as cloud storage of cloud technologies.

Key words: Cloud storage, data privacy, hybrid encryption, blockchain, public key, Cipher-texts

INTRODUCTION

Ryan (2013) defined the cloud computing as "an idea that data and programs can be stored centrally in the cloud and accessed anytime from anywhere through thin clients and lightweight mobile devices." Cloud computing is based on accessing resources via. the internet. The cloud computing follows a simple "Pay as You Go (PAYG) Model" where you pay for the services you've used (Subashini and Kavitha, 2011). In 2006 Amazon company provided Amazon Web Services (AWS) for cloud users to offer enormous computational speed with minimum expanse on software and hardware (Varia and Mathew, 2014). Since then, large companies have started to adopt the idea of cloud computing and provide users with different innovative services in this domain. According to IDC, the total spending for the deployment of cloud environments have increased by 15.5% reaching $37.5 billion in 2016 (Patidar *et al*., 2012).

IBM forecasted 60% more deployments by big organizations that are ready to embrace cloud computing in the next few years (Horjan, 2011). Based on root architecture, the cloud services are divided into three models namely: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) and four deployment models namely: public, private, hybrid and community cloud. Despite the increasing potential of cloud-computing, its models are still facing critical challenges, expressed as the absence of standards and user's privacy preservation (Jansen, 2011).

That is why numerous organizations are reluctant to fully leverage the benefits of the cloud. Individuals and organizations are still reluctant to fully rely on cloud providers citing concerns about data privacy and reliability and highlighting the risk of data privacy and unauthorized access. Encryption is a common data securing technique to mitigate privacy risk on the cloud and to provide sound confidentiality against external attacks (Almasri *et al*., 2018). However, the encryption techniques have been proved inefficient to protect data against corruption caused due to configuration errors and software bugs like data theft or manipulation of data within the data center as data is usually encrypted by rogue employees or attackers within the machines of the cloud provider.

Now a days researchers are exploring deploying blockchain to address the security challenges of the cloud. The most successful usage of blockchain was building cryptocurrencies that experienced a sudden and unexpected price surge in 2018 and demanded the need for different and novel data security technologies. The blockchain is essentially a distributed database of a public

Corresponding Author: Marwan Adnan Darwish, Malaysian Institute of Information Technology, University Kuala Lumpur, 1016 Jalan Sultan Ismail, 50200 Kuala Lumpur, Malaysia, Marwan.khabbaz1@gmail.com

ledger of all transactions or digital events executed and shared among participates (Zikratov *et al*., 2017). Each transaction in the public ledger is verified by consensus among a majority of the participants in the system. Once entered, information can never be erased and modified (Rifi *et al*., 2017). The blockchain stores verifiable record of every single transaction ever made. Beyond currency, the blockchain can be used in smart contracts, record keeping, ID systems, cloud storage infrastructure and various trust based systems of information technology and industry domains (Lin *et al*., 2018). Blockchain technology is an ordered composition of blocks that store the data records. Every block consists of the header that includes a hash, transactions, timestamp with proof of work to link the block with a hash of previous one block.

The hash is resistant to decrypt the result of the block transactions. The genesis block is the first block to refer the entire blockchain, i.e., hardcoded into the applications and it doesn't reference any previous block. If the block will be added then all node sends the result of the connected unit to others if there are no errors, then the block will be added and included the hash of the previous one (Raju *et al*., 2017).

This technology is under research in all industrial domains because it's amenities features (Ali *et al*., 2018) like, user isolation, scaling, tamper-proof, decentralized structure, immutability, transparency, cohesion, event based-trigger, modular core. In our study, we are exploring its potential for cloud privacy and data integrity using blockchain technology (Liu and Xu, 2018). Figure 1 conceptualize the use of distributed ledger for the cloud.

Literature review: Lin *et al*. (2018) proposed a scheme to avoid shortcomings from using public-key certificates. The scheme is secure against forgery of messages fabrication and ID attacks by applying ID-based linearly homomorphic signature under the random oracle model using blockchain technology (Lin *et al*., 2018).

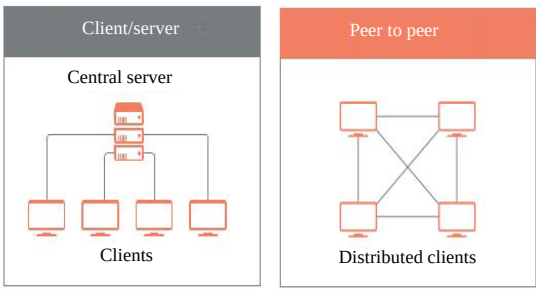

Fig. 1: Distributed ledger for cloud

Using blockchain (Zikratov *et al*., 2017) did another attempt to ensure the data integrity against misused attempts and to reduce the data threats by implementing well-formed transaction authentications and audits. This is to achieve the security attributes like confidentiality and availability and to find a lightweight technique rather than MAC that algorithms which need two inputs a secret key and variable for data length and this algorithm will be held on the client-side to calculate the value and outsource the data on the cloud and whenever the data owner wants to check the integrity he will download again and compare the value of MAC and this process will add more computational cost and bandwidth for large file, so, the blockchain will be the best replacement solution for integrity (Zikratov *et al*., 2017).

Another new approach proposed by sukhodolskiy for data control that has been stored inside the cloud environment without any third-party participation via. blockchain-based access control system to solve the problem of customized access on data without duplication among a large number of participates of cloud storage services (Sukhodolskiy and Zapechnikov, 2018). Rifi *et al*. (2017) proposed a technology to protect the IOT access using blockchain technology, the critical problem for the e-Health smart homes to manage the huge data from monitoring the diseases for elderly and immediately send it to a single server. This centralized structure will face lots of problems to process this magnitude of data with a transparent and secure way, so, the blockchain proved itself as an efficient way to process the data seamlessly (Rifi *et al*., 2017).

Raju *et al*. (2017) have proposed a privacy-enhance system for user identity management using blockchain that enables network access with pseudonymous identities and hinders the reconstruction of subscriber's identities. Liang *et al*. (2017) proposed a ProvChain architecture to verify and detect cloud data provenance embedding the transactions into the blockchain. It comprises of contains three main phases, provenance data collection, provenance data storage and provenance data validation. To preserve user-privacy and tamper-proof data provenance blockchain is used for validation procedures and generate a receipt of each record (Liang *et al*., 2017).

Puthal *et al*. (2018) applied the decentralized framework of blockchain to ensure data security and validity. In this research, we are applying the public key encryption algorithm to ensure user data privacy at the cloud infrastructure.

MATERIALS AND METHODS

To overcome the privacy risk of traditional data handling method of cloud with encryption only at client

side like boxcryptor or client-end-encryption such as in SpiderOak, the proposed research suggests encrypting the data at server end using enhanced public key encryption. Here, the blockchain technology is adopted at cloud server to authenticate and validate the cipher data.

The proposed model delegates the key management and control to the clients. To our knowledge from the literature review, the existing cloud models are not leveraging the full benefit of storing only encrypted data at server end while maintaining the key management at the client end. The proposed framework illustrates how data can be encrypted while storing and decrypted while retrieving within IaaS and maintaining the key management as SaaS. It facilitates and maintains the data integrity for the whole encryption/decryption cycle.

The framework is built as a virtual layer over the cloud infrastructure. This cloud storage comprises of virtual machines resembling Infrastructure as a Service (IaaS). It enables cloud providers to maintain an efficient and flexible cloud for clients with all benefits and features (privacy preservation, cost reduction, all times backup, easy deployment and maintenance). The next trend in the virtualization in IT is NFV (Network Function Virtualization) which was derived from SDN (software-defined networking). SDN is the latest approach to networking that eliminates the complex and non-dynamic (static) nature of legacy distributed network architectures through the use of standards-based software abstraction between the network control plane and underlying data plane including both virtual device and physical ones. The NFVI functional block in the architecture has three domains (Anonymus, 2016): compute domain {This domain includes the computing and storage resources that provide processing and storage to VNFs through the virtualization layer (e.g., hypervisor).} that includes computing and storage resources that are commonly pooled. Virtualization domain that includes the virtualization layer for VMs and containers that abstracts the hardware resources and decouples the VNF from the underlying hardware. Infrastructure networking domain that includes both physical and virtual networking resources that interconnect the computing and storage resources.

Figure 2 illustrates the NFV infrastructure. Most of the modern cloud data centers are equipped with virtualized clusters, running hypervisors on virtualization supported hardware (Zhang and Meddahi, 2017). Intrusion Detection Systems (IDS) is a software that monitors and detect any malicious behaviors using SIEM (Security Information and Event Management), firewall is a security system designed to prevent the unauthorized uses and load balancer is used to manage the load over the networks. Due to the flexibility and timely availability of desired resources, these services are run on the

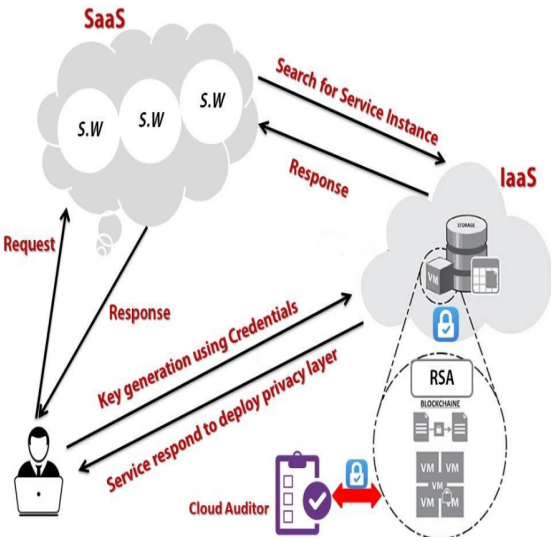

Fig. 2: Proposed framework

virtual domain inside the cloud infrastructure. This framework integrates the privacy layer (encryption/decryption layer) inside the cloud storage to enhance the privacy of users and companies seeking cloud services. The big idea here is to build a server end encryption along with user management keys, then the pair of keys will be unique for each user and different from the others after generating them from the user credential at the client side, far from the service provider in order to add more privacy to the clients.

The encryption layer is launched in IaaS (third service model in cloud computing). Depending on the encryption keys, the sensitive and secret data will be encrypted with a hybrid algorithm including AES (advanced encryption standard) and RSA (Rivest Shamir Adleman). The data, then will be encrypted before being stored in the data center and will be secured as only the user can decrypt it with his pair of keys. After the encryption is done, blockchain technology is deployed to verify data integrity by comparing the digital signature from every single transaction that belongs to the user. The digital signature will be stored after hashing the encrypted data inside the transaction set in the block.

One of the most important added value in this study is incorporating a decentralized data structure by using blockchain to create multiple copies for every node which are managed by cloud auditors to validate the encryption/decryption process, so, data integrity is achieved after the completion of the encryption process. In contrast, the downloading process is reverse to the latter one in which the service will decrypt the data when the user wishes to download on the local device using the decryption phase with the private key. Figure 2 explains the proposed framework in details.

The method is of twofold: the frontend (users) and admin (cloud service providers). The frontend consists of the programs that been provided by cloud providers. The admin is responsible for processing the transactions, creating blocks, checking blockchain and handling all user access control. Our method is divided into two main parts:

Frontend: The user interface is a web application which provides the user the ability to access the provided storage space (uploading/ downloading data). There is a privacy layer before storing/uploading data into the machines that encrypt the data using a newly hybrid algorithm and decrypt data after downloading the data from the cloud. The algorithm will randomly generate the pair keys (public key for encryption and a private one for decryption) using the user credentials as a seed.

Backend: The backend is the core of our system. It is where the blockchain is implemented. The blocks are going to store the encrypted data after hashing it into fixed length to store in transaction part with block hash, timestamp and proof of research. The admin has the right to check the data integrity for the chain by comparing the signature that hashed from the encrypted data to the transaction metadata to make sure of data protection.

Blockchain based hybrid algorithm: A newly blockchain based hybrid algorithm is developed for building the privacy layer and integrate it with the cloud infrastructure. The main steps included here are the key generation and using a hashing function on blockchain. Hash is generated of the user's passphrase using the SHA256 algorithm found at webtoolkit.info. This hash is used to seed a random number generator. A (seeded) random RSA key is generated with RSA key generator as a hard-coded public exponent. Furthermore, a 32-byte AES key is generated with RBG (Random number Generator) for the encryption process. The plaintext message is converted to a byte string and padded with zeros to 16 bytes around. An initialization vector is created with RBG random number generator.

In addition, the AES key is expanded and the plaintext message is encrypted with the Cipher-block chaining mode using the Jsaes library. The AES key is encrypted with the recipient's public key using RSA encryption library. RSA: is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". And this algorithm is going to used inside the privacy layer to generate and encrypt/decrypt the data.

Also with AES (Advanced Encryption Standard) the symmetric algorithm that uses only one key for encryption and decryption to help with the acceleration of the algorithm to get the best results in short time. So, the encryption process will be done by AES and to secure the symmetric key of the algorithm by using RSA algorithm. SHA-256 cryptographic hash algorithm: A cryptographic hash (sometimes called 'digest') is a kind of 'signature' for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. A hash is not 'encryption' it cannot be decrypted back to the original text (it is a 'one-way' cryptographic function and is a fixed size for any size of source text).

This makes it suitable when it is appropriate to compare 'hashed' versions of texts as opposed to decrypting the text to obtain the original version. In the end, blockchain technology: hashing means taking an input string of any length and giving out an output of a fixed length. In the context of cryptocurrencies like Bitcoin and run through a hashing algorithm (Bitcoin uses SHA-256) which gives an output of a fixed length and store the data into the transaction set and each block linked with the others by block's hashes.

System implementation: A simulation was carried out to illustrate the system implementation starting from user sign up and ending with the core of our system using Blockchain technology. A cloud auditor is built using PHP 5.6+JavaScript, ES5 and MySQL database to monitor the matching between the transactions data within the blocks and the encrypted data within the data centre of the cloud.

Phase 1: A privacy service is added to the user interface at the users end to generate unique keys for each user using the credential on the SaaS service model. In order for the service to be deployed at the virtual machine, both public and the private keys are generated and merged within the privacy layer to encrypt or decrypt the data according to on demand service.

Phase 2: In this phase, chain of blocks was built at the server end. The blocks at IaaS provides a decentralized structure of the cloud platform. This is critical for the hashing functions since the digital signature is generated and stored within the blocks according to the time stamp. Having the data stored in blocks allow the system to carry out an automatic matching process that keeps comparing the content of the encrypted data with its digital signature. Figure 3 shows the technology of blockchain.

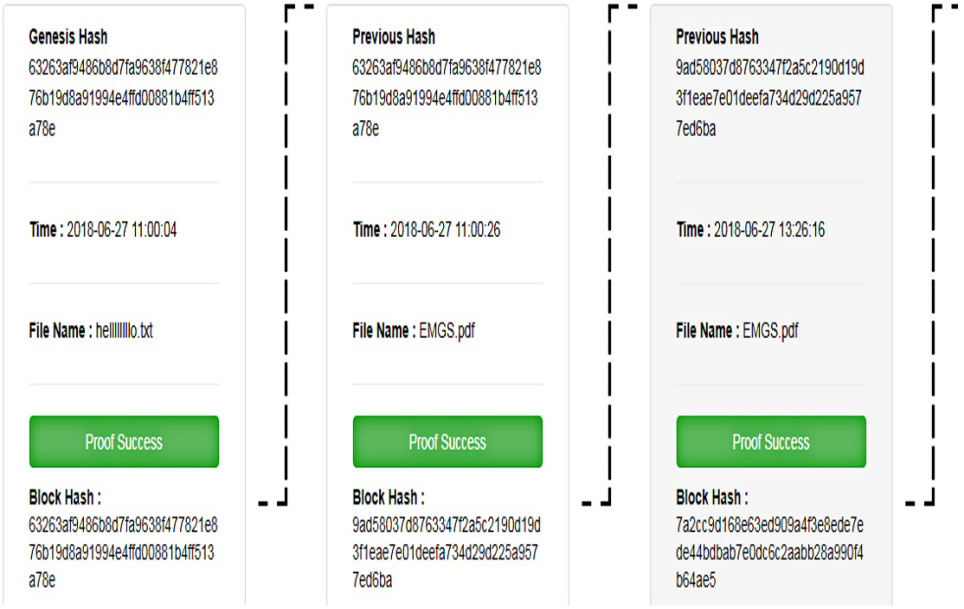

Fig. 3: Blockchain technology

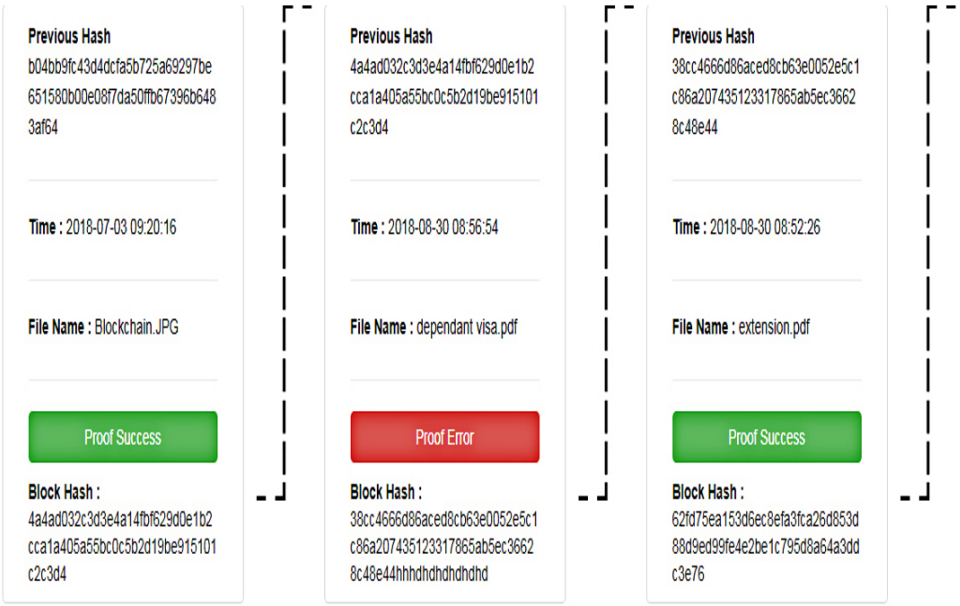

Fig. 4: Error detection using blockchain

Phase 3: In this phase, various malicious attacks within the cloud storage were carried out to test the efficiency of the system. One specific example of an attack is presented here in which data modification was performed. The proposed matching algorithm successfully highlighted the ruined block after finding discrepancy between the encrypted data and this specific digital signature. This is vital for the cloud auditor to monitor the integrity and reliability of data at the cloud. Figure 4 illustrates the detection of the attack.

Phase 4: At the end, an encrypted database, similar to what actual cloud providers has is built at the infrastructure layer. This conceptualizes a new framework for storing records. Data is secured and encrypted and the keys for accessing the data belongs exclusively to the

image	user_id	signature	created
OoTKcngEYUC7N5/krapKvtUHyUyaCwG9uqhx+A+Kgsly4oHc8m...	1	63263af9486b8d7fa9638f477821e876b19d8a91994e4ffd00...	2018-06-27 11:00:04
CmsczgenQvUDWDB1ZEI7UnAV6zKy4w30Ipvy+nqVbRoDS6UEUl...	1	9ad58037d8763347f2a5c2190d19d3f1eae7e01deefa734d29...	2018-06-27 11:00:26
CM7sDJD7XK/UnE4Hhy5oO2f+arjW47n+MbZIvNhSIw2jzfEMGF...	1	7a2cc9d168e63ed909a4f3e8ede7ede44bdbab7e0dc6c2aabb...	2018-06-27 13:26:16
CM7sDJD7XK/UnE4Hhy5oO2f+arjW47n+MbZIvNhSIw2jzfEMGF...	1	00fc7db2c0cf8418fcf2972723e7d34783fb24d039300d5f38...	2018-06-27 13:27:44
pGDbB687AwPNLjhI3MJvJILZQ+VYo9LIdH4CCgH2zhrOkzpfeS...	1	ee166d4b77cf04bbe7f4d5419774f78c752e6478f7927ea93b...	2018-06-29 06:41:29
cI3fkTLzXID1IPV+Q4d5wM9IWpFTSL3kQBskSl6jORYtWaOC5s...	1	b04bb9fc43d4dcfa5b725a69297be651580b00e08f7da50ffb...	2018-07-03 09:19:18
EZ0suFjvEEvlv83tkes8RzodNtsXoy7uor/kEQUdMuM71F1h0g...	1	4a4ad032c3d3e4a14fbf629d0e1b2cca1a405a55bc0c5b2d19...	2018-07-03 09:20:16
MaM44+Koy0uWiNLyNHY5FOszG+HIAp6JIs+jJxR7SvQXERYAr+...	1	38cc4666d86aced8cb63e0052e5c1c86a207435123317865ab...	2018-08-30 08:56:54
Rli5X1hi86X3A3OP4kB1wwkQjzB5NPvZaRRIkkGY3TwEgwXe3l...	2	62fd75ea153d6ec8efa3fca26d853d88d9ed99fe4e2be1c795...	2018-08-30 08:52:26
nmL3Jb1Q/I3JOGkg4kZXHVoo9F+BY/IfyL703Utaok5A16XHRg...	1	965d195d9478bad7674ba5545cd7bfa54deacbc7d75d53a257...	2018-08-30 17:09:03

Fig. 5: Encrypted database

data owners. In other words, data is far from cloud provider's unauthorized uses. Figure 5 shows the new framework of encrypted data.

RESULTS AND DISCUSSION

In this study, the extracted results from the simulation environment highlight the development of the data privacy inside the cloud storage infrastructure comparing with previous providers. The privacy level performance that has given from the proposed framework is shown in Fig. 6. The framework preserves the data privacy of 97% from data center when the hackers or adversaries are active in the system because the system can detect the changes of the stored data by using blockchain checking hash-codes concept to validate the data integrity and privacy.

Furthermore, the experiment by using 1000 attacks using an automated open source tool used to simulate and visualize the posture of the cloud infrastructure with different data sizes then corrupt the data by stealing or tempering the encrypted data trying to figure out the origin of data. This attribute wasn't applied before at the traditional cloud environment.

In addition, the proposed framework could overcome with different kinds of attacks: Man-in-the-Middle attack (MITM): where attacker based between the two sides of communication which are the clients and the CSP (Cloud Service Provider) trying to expose the data and steal the sensitive data from the clients. Whereas the attacker impersonated the second party and made an independent connection to convince the remaining parties to send the messages directly. The proposed framework prevents this kind of attacks because the sensitive data will be in encrypted form using hybrid cryptosystem that contains AES for the whole process and RSA for key distribution

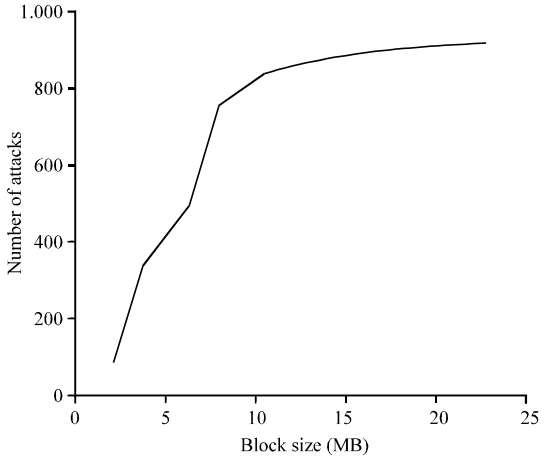

Fig. 6: Privacy level

management, so, the attackers can't reverse the cipher data into the original one and the architecture of the blockchain which use the authentication using transaction ID between the both side to secure the communication.

Distributed Denial of Service (DDOS): That used various malicious or Trojans to exploit data and to infect the system's resources, controlled by the hackers. This attack is one of the most common attacks in the cyber threats in the IT field. The framework will eliminate this attack because of the hierarchical of the methodology by using blockchain technology as a distributed data structure with smart contracts. Smart-contract like, matching hash ID and authenticating the TX-ID and these contracts can't be accessed physically.

Cloud Service Provider (CSP): The third party that controls the data in behalf of the users and may use this

data for unauthorized purposes like commercializing profits and selling for other companies because the data will present in clear form without any obfuscation attempt in the cloud server machines. So, the data will be in encrypted with the hybrid algorithm with non-readable way. Then, it will be far from the provider's hands and achieve the privacy goal.

CONCLUSION

The vast development of information and communication technologies in recent years lead to embracing cloud computing and cloud providers more than before. However, data privacy and security remain the utmost challenges of users and companies. Traditional encryption alone will stay weak against different types of bugs and glitches inside the system. To address those challenges, we proposed a Blockchain based hybrid algorithm. The algorithm was built above a blockchain system that combined AES+RSA, one for the encryption and decryption and the other for ciphering AES key to rapid the performance and make it more robust against the attacks.

The system was deployed at the privacy layer of a locally built cloud for increasing the level of privacy and reliability and ensuring data integrity. The blockchain is the new technology that has the potential to contribute positively to data privacy and integrity. The results proved that blockchain is able to create strong trust, transparency and responsibility between the users and cloud providers. It has the potential to change the whole internet process and revolutionize the way of information security in different types of industries.

REFERENCES

Ali, J., T. Ali, S. Musa and A. Zahrani, 2018. Towards secure IoT communication with smart contracts in a blockchain infrastructure. Intl. J. Adv. Comput. Sci. Appl., 9: 584-591.

Almasri, A.H., M.F. Zuhairi, M.A. Darwish and E. Yafi, 2018. Privacy and security of cloud computing: A comprehensive review of techniques and challenges. Intl. J. Eng. Technol., 7: 240-246.

Anonymus, 2016. SDN-NFV reference architecture. Verizon Wireless Telecommunications Company, New York, USA. https://www.slideshare.net/Netmanias/verizon-sdn-nfvreferencearchitecture

Horjan, J., 2011. The Essential CIO. IBM Corporation, Armonk, New York, USA.,.

Jansen, W.A., 2011. Cloud hooks: Security and privacy issues in cloud computing. Proceedings of the 44th Hawaii International Conference on System Sciences, January 4-7, 2011, Kauai, HI., USA., pp: 1-10.

Liang, X., S. Shetty, D. Tosh, C. Kamhoua and K. Kwiat *et al*., 2017. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, May 14-17, 2017, IEEE Press, Madrid, Spain, ISBN:978-1-5090-6610-0, pp: 468-477.

Lin, Q., H. Yan, Z. Huang, W. Chen and J. Shen *et al*., 2018. An ID-based linearly homomorphic signature scheme and its application in blockchain. IEEE. Access, 6: 20632-20640.

Liu, L. and B. Xu, 2018. Research on information security technology based on blockchain. Proceedings of the 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), April 20-22, 2018, IEEE, Chengdu, China, ISBN:978-1-5386-4302-0, pp: 380-384.

Patidar, S., D. Rane and P. Jain, 2012. A survey paper on cloud computing. Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies (ACCT), January 7-8, 2012, IEEE, New York, USA., pp: 394-398.

Puthal, D., N. Malik, S.P. Mohanty, E. Kougianos and C. Yang, 2018. The blockchain as a decentralized security framework [future directions]. IEEE. Consum. Electron. Mag., 7: 18-21.

Raju, S., S. Boddepalli, N. Choudhury, Q. Yan and J.S. Deogun, 2017. Design and analysis of elastic handoff in cognitive cellular networks. Proceedings of the 2017 IEEE International Conference on Communications (ICC), May 21-25, 2017, IEEE, Paris, France, ISBN:978-1-4673-9000-2, pp: 1-6.

Rifi, N., E. Rachkidi, N. Agoulmine and N.C. Taher, 2017. Towards using blockchain technology for IoT data access protection. Proceedings of the 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), September 12-15, 2017, IEEE, Salamanca, Spain, ISBN:978-1-5090-5008-6, pp: 1-5.

Ryan, M.D., 2013. Cloud computing security: The scientific challenge and a survey of solutions. J. Syst. Software, 86: 2263-2268.

Subashini, S. and V. Kavitha, 2011. A survey on security issues in service delivery models of cloud computing. J. Network Comput. Appl., 34: 1-11.

Sukhodolskiy, I. and S. Zapechnikov, 2018. A blockchain-based access control system for cloud storage. Proceedings of the 2018 IEEE International Conference on Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), January 29-Feburary 1, 2018, IEEE, Moscow, Russia, ISBN:978-1-5386-4339-6, pp: 1575-1578.

Varia, J. and S. Mathew, 2014. Overview of amazon web services. Amazon Web Serv., 1: 1-22.

Zhang, Z. and A. Meddahi, 2017. Security in Network Functions Virtualization. Elsevier, Amsterdam, Netherlands, ISBN:9780081023716, Pages: 272.

Zikratov, I., A. Kuzmin, V. Akimenko, V. Niculichev and L. Yalansky, 2017. Ensuring data integrity using blockchain technology. Proceedings of the 2017 20th International Conference on Open Innovations Association (FRUCT), April 3-7, 2017, IEEE, St. Petersburg, Russia, ISBN:978-1-5090-6487-8, pp: 534-539.