ToSSecC: Two-Stage Solution for Securing Cloud Data Using Game Theory

Ashis Kumar Samanta
Department of Computer Science and Engineering
University of Calcutta
Kolkata, India
Orcid ID: 0000-0002-3031-4225

Nabendu Chaki
Department of Computer Science and Engineering
University of Calcutta
Kolkata, India
Orcid ID: 0000-0003-3242-680X

2021 International Conference on Data Analytics for Business and Industry (ICDABI) | 978-1-6654-1656-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICDABI53623.2021.9655810

Abstract—The use of the cloud for storing data for online applications has become a popular technology. It has become a paradigm of the next generation. With the widespread of smartphones and popular applications like Facebook, WhatsApp, etc., individuals are much acquainted using cloud storage, even without understanding the same. However, the security of data in the cloud is still a big issue irrespective of the user and cloud provider. Applications are implemented in various domains to achieve data security, privacy, and data transparency in cloud-based applications. The evaluation of smart contracts, run on the blockchain framework, is used nowadays in diverse sectors of business for achieving data security. However, in real-life implementation, it is found that the blockchain itself is suffering from different security threats. In this paper, a methodology, ToSSecC is proposed towards enhancing the security features of cloud data by addressing the issues of spam mails in the admission system of a large university in India. The work has been divided into two steps: 1) Deployment of in the cloud-based application, by incorporating smart contract and 2) Enhancement of the security of the smart contract by proper validation using game theory.

Keywords—Blockchain Application, Smart Contract, Data Security, Game Theory, Email Security

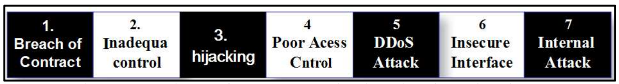
I. INTRODUCTION

The application support along with the infrastructural support over the internet with reduced cost and handling hazards attracts the people to explore the data and business in a distributed environment, which is the facility of the cloud computing environment. The service support of the cloud is rendered to the cloud customer on a demand basis. The cloud control is shared among different vendors; therefore cloud data always remain under high-security risk [8]. Cryptography and cloud-enabled technology were introduced into the world to secure cloud data. The blockchain has already explored its research wings in different domains of online transactions of day-to-day applications. It is a distributed, peer-to-peer, tamperproof, cryptography-based network that maintains a hash key for every transaction [1]. Though the initial concept of distributing the data in a public network, due to the requirement of the application the private and consortium has also been incorporated in many of the applications, and many consensus algorithms are used to secure the data transactions [2]. Though has a lot of potentials to build up real-time applications, still it has some limitations because it is still in its initial stage of research and development.

The objective of this paper is to analyze the security issues of cloud storage and the solution, ToSSecC is proposed incorporating smart contracts for applications. On the other hand, the smart contract, and itself have some security vulnerabilities and these are addressed in this work using game theory.

II. EXISTING SECURITY ISSUES OF CLOUD TECHNOLOGY

The setting of the same cloud is shared to different cloud customers by the cloud vendor. That makes the security of the cloud vulnerable. The popularity of the use of clouds has increased the number of times and different security solutions were also proposed, but new security threats are generated to make the cloud vulnerable. The security threats that make the cloud insecure are described below (Figure. 1).



1. Breach of Contract	2. Inadequa control	3. hijacking	4 Poor Acess Cntrol	5 DDoS Attack	6 Insecure Interface	7 Internal Attack

Fig. 1. Matrices of IssuesSecurity in Cloud Technology

Breach of contract: The huge amount of corporate data is stored in the server of the cloud. In case of any intention to damage the brand value or lass in business, the cloud vendor has the pointed specific target [8].

Inadequate Control: The cloud provider offer the cloud space without developing the control solutions to secure fro the risk factor from many operations in many sectors [4].

Hijacking: The attacker may use the available cloud environment for exploitation in software, exploitation in data, or any kind of fraud [8].

Poor Acess Control: The poor access control module provided by the clouds many times brings up attacker security threats[4].

Dynamic Denial of Service(DDoS) Attack: The efficiency and the performance of the application gets slowed down to get access to the application by the attacker[3].

Insecure Interface: The store and retrieve of data from the application to the cloud is done by the API interface. Improper security testing would generate a high risk of security threats[4].

Internal Attack: This kind of attack is coming from the internal users of the application, other cloud share partners, or the vendor itself by deleting data or access control[3].

III. LITERATURE REVIEW

In this section, we try to select the literature on the application of in various domains to explore the fact that how this technology improves efficiency and generates trustworthiness in the respective application. We also want to see the extent that the blockchain implementation provides the solution to the existing issues, whether that implementation raised some new challenges.

In paper [2], proposed an application of patent ownership and copy-right issues using blockchain technology. The application deals with the payment of royalty for copyright documents due to data authorization and data security problems by securing the IP address with the "InterPlanetary File System (IPFS)". The idea is valuable, the methodology of implementation of the customized through three layers by its efficiency is not properly highlighted. The tamper-proof data security properly authenticates it by the authorized node and makes the copy-right certificate available through a distributed network. The author is also silent about the cost incurred by the application. A "Game strategical Block" is proposed by the authors in the paper [3] to prevent cloud security attacks. An application has been proposed in [5] on the issuance of a "Certificate of Digital Signature" through the blockchain method using "Public Key Interface (PKI)". The record of the individuals is kept in encrypted form, for future use which is hard to tamper with. An application of patent ownership and copy-right issues is proposed that uses blockchain technology to pay the royalty for copyright documents with proper data authorization and data security. The author in paper [6], has proposed the security solution to adopt blockchain applications in the cloud environment. The "proof of concept" is incorporated to secure the data of service level agreement of cloud users and vendors using the smart contract.

A blockchain-based microservice system to support the examination processing is proposed in [7] to enhance security. The author emphasis incorporating private blockchain technology to address the existing problems of security and trust. The author calculated the efficiency factor and claimed about the system has better throughput and low latency. The incurred cost is not discussed. The author of the paper [8], proposed a protocol that the miner will decide to allocate their resources to mine the transactions of different cryptocurrencies to gain maximum. In paper [9], it is stated about the group-key generation and authentication of the group member to communicate among the members of the mobile group. In most cases, the protocol does not function properly. The author of this paper proposed a protocol dynamic protocol that would maintain privacy, performance, and security to communicate among the group member and also to trace the members who are involved in malicious activities. In paper [10], the author proposed a two-phase sharing co-operative game theory model to eliminate the computation overhead. In the first phase of the proposal, the total number of transactions in a period is shared among the nodes within the network for validation. The share-based nodes then validated the transactions accordingly. The author also claimed and shown in the simulating result that the efficiency in their two-phase consensus game protocol is much better than some of the existing works. The security issues of mobile cloud computing and the security models developed by the researchers are analyzed by the authors in the paper [11]. In paper [12], the author developed and analyzed a model of security system in the education domain and interpreted the result of threats generated in the system in case of using untrained human resources in the information technology desk.

The study of applications on various domains provides us a concept that this technology mainly incorporated for the security of data and transactions. The actual existing issues of applications and directions for future research are discussed in the following sections.

A. *Findings and Gap Analysis*

The main focus of healthcare and most of the other applications is to use the immutable and distributed network property of the private-public. The cost of a particular type of treatment can be shared within the network. How the entire process will be helpful from the patient end as the access right of the private network is not mentioned in the paper. It is not mentioned also whether the operative cost will be reduced.

The risk of IoT interface application has two aspects. First, the accuracy of the data depends upon the sensitivity of the IoT devices. Secondly, the quality of the data depends upon the degree of interfacing of the IoT devices with the blockchain.

The random selection of the nodes to enhance the performance of the security threat is compromised due to the selection of dishonest nodes in the paper [10].

The theoretical concept and the practical implementation of blockchain have left a huge gap regarding its existing issues and solutions. Almost all of the applications mentioned above have not mentioned the

- The security issues of the cloud still make the cloud vulnerable.
- The secure blockchain also suffering from different security issues. None of the applications have provided any measures to upgrade the security features.
- How does the blockchain can provide a better solution to these issues?

B. *Problem Definitions*

In the Existing system (Figure 2) the university has a portal for student admission. The entire system is run in the cloud. The following steps are involved in the existing system.

1. The applicant who is the user (student), applies for various courses of M.Tech, B.Tech, M.Sc, M.A, LL.B, etc. It is normally seen that the university received near about 70000(seventy thousand) applications per year.
2. In the due course of application, the applicants (students) first register into the portal, and then a "One Time Password (OTP)" is sent to the students mentioned emailed, and after verification of OTP, students are registered and let to login to the network of the portal.

3. After logging into the portal the student can send the relevant data and information required for admission and also can upload other necessary documents.

The university wants to verify the email because of future communication and also the issue that the students have not provided any unused or unauthorized email to avoid any sort of legal litigation. The university hires the application server, data server, and mail server which are maintained in the cloud by the vendor. The email account(xyz@univ.in say) is provided by the domain server on behalf of the university to communicate with the students by email.

The applicants submit the applications with relevant data after login into the portal. After the submission of data by the students, the applicant acknowledges accordingly attached with an application report (called application form) to the email address provided. The acknowledgment email is initiated by the mail server hired by the university from the university designated email account xyz@univ.in.

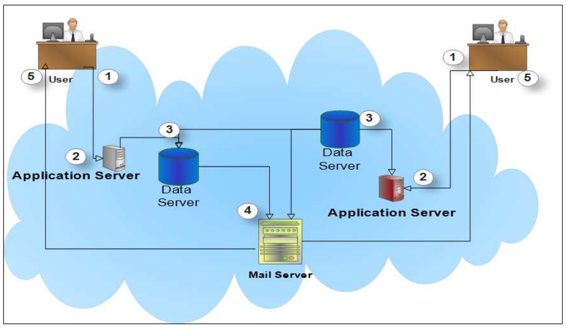
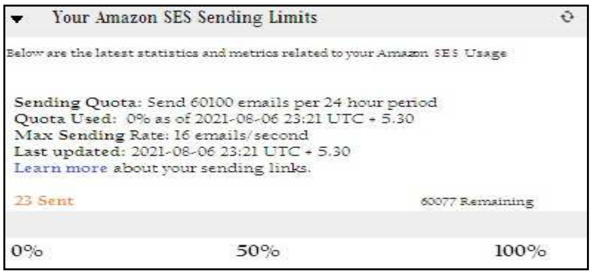


Fig. 2. Existing University Admission System in Cloud

The initial condition of the mail server provided by the vendor is “For best results, maintain a bounce rate below 5%. Higher bounce rates can impact the delivery of your emails. If your bounce rate is 4% or greater, we automatically place your account under review. If your bounce rate is 8% or greater, we might pause your account's ability to send additional email until you resolve the issue that caused the high bounce rate”.

Some security holes are evident in the existing admission application system, and also in the cloud system, by which spammers can access the forms of application that are responsible for sending emails and generating the SPAM emails. In 24 hours, observed during this study, a total of 58,292 emails were sent including those due to the SPAM activity. Due to the presence of a huge amount of spam emails, the email account of the university is paused, In turn, the true applicants could not understand whether their applications had been submitted properly and were confused. Subsequently, they have tried with the repeated application attempts leading to the generation of several duplicate applications, and thus affecting the entire admission process. It is found from the spamming email, that the address of the email is sent which is the accumulation of the following formula. (Applicant email).(date).(continuous number)@domain name. **Example:**gurmit.8.08.2021.000001@gmail.com



Your Amazon SES Sending Limits

Below are the latest statistics and metrics related to your Amazon SES Usage

Sending Quota: Send 60100 emails per 24 hour period
Quota Used: 0% as of 2021-08-06 23:21 UTC + 5.30
Max Sending Rate: 16 emails/second
Last updated: 2021-08-06 23:21 UTC + 5.30
Learn more about your sending links.

23 Sent
60077 Remaining

0%
50%
100%

Fig. 3. Spamming Email Report of Cloud Vendor

In this paper, this issue is addressed to secure the data in cloud systems by using blockchain, smart contract, and game theory as well.

IV. THE PROPOSED METHODOLOGY

A. Hypothesis and Assumptions

The assumptions are taken in this case that two players are participating in the game, one is a normal user (honest user) and the other is the attacker. Both the user bears a logical sense and can take logical strategies within the given set of strategies. The players either do nothing or attack. If the honest user attacks the dishonest user, then the honest user proactively increasing his security domain. The attacker attacks the system to damage the system and hack some important information. The sum of the probability of attack and not attack is always 1.

B. Two-stage Solution for Securing Cloud Data (ToSSecC)

The proposed Two-stage Solution towards Securing Cloud (ToSSecC), is presented in this section with a running case study on the university admission system. In the first stage, it is recommended to incorporate the university admission system. The utility of the application is that the data would be tamper-resistant and immutable. This increases the trustworthiness of data.

In the second stage of ToSSecC, with the incorporation of a smart contract facility between the applicant and the university, the system would be more document-free, fast, and secure data storage where the privacy of the data can be maintained. In this solution, we developed a smart contract application using for the incorporation of a private admission system.

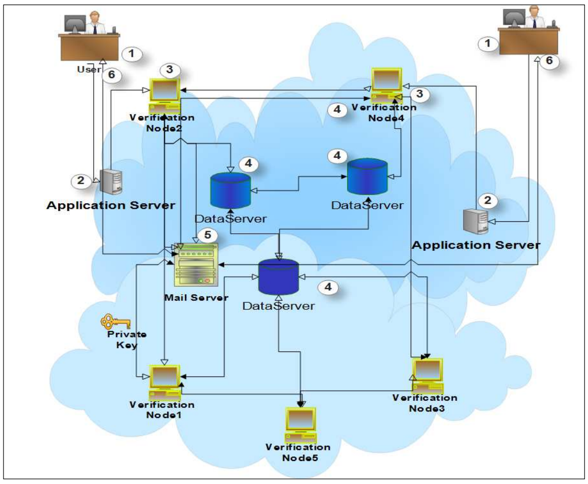


Fig. 4. Smart Contract Application of Admission System

TABLE I. SYMBOL USED

n	The average number of applicants (block) in a time interval
m	Number of applicants data(block) accessed by the attacker
p_h	Probability of verification of honest node
P_a	Probability of verification of attacker
H	Total hash power used in the system in the same interval

In the application system there are two possibilities either attack with probability P_a ($P_a \geq P_h$) or not attack with probability P_h ($P_a < P_h$). in case of attack, the number of nodes dishonestly verified and mined by the attacker is

$$\text{n'} = \begin{cases} m \ when\, p_a \geq \ p_h \\ n - m \ when\, p_a < p_h \end{cases} \text{..........................(1)}$$

The probability is calculated by poiso distribution($\lambda = np_h$)

$$p_a = \frac{e^{-\lambda} \times \lambda^m}{m!} \text{ and } p_h = (1 - p_a) \text{......................(2)}$$

If the attacker is successful to attack the system or mail server ($P_a \geq P_h$) and does not attack the server ($P_a < P_h$) then the function becomes

$$F_a(\text{m} \mid \text{n}) \ = \ p_a \times H \ - \ p_h \ \times H \ldots when\, p_a \geq \ p_h.\text{(3)}$$

$$F_h(\text{m} \mid \text{n}) \ = \ p_h \times H \ - \ \ p_a \ \times H \ldots when\, p_a < p_h \ \text{(4)}$$

Therefore, there may be four situations that can be raised in this system, that the honest node and the attacker both can go for not attack each other, one can attack the other or both can attack each other. The payoff is shown in Table II. If the attacker does not attack then the entire hash value shall be utilized for the validation and mining of the data for the honest node irrespective of the attack or the honest node.

TABLE II. THE PAY-OFF MATRIX OF THE GAME

		The attacker (A)	
		Honest	***Attack***
Honest user(H)	***H***	$\{p_h H,\ p_a H\}$	$\{p_h H,\ F_a(\text{M} \mid \text{N})\,\text{H}\}$
	A	$\{F_h(\text{M} \mid \text{N})H,\ p_a H\}$	$\{F_h(\text{M} \mid \text{N})\,\text{H},\ F_a(\text{M} \mid \text{N})\text{H}\}$

In a real-life situation, it is not expected that an attacker would not attack. In the problem definition, it is a clear indication from the vendor that to get under the review, the bounce rate of email would be 4% or greater and the email account automatically paused if the bounce rate of email is 8% or greater. Therefore, there may be situations that can be chosen for the probability rate of the attacker for SPAM email.

$$p_a\ is \begin{cases} < 4\%\ to\ protect\ \ system\ for\ the\ case\ of\ noattack\ for\ SPAM \\ \geq 4\%\ and < \ 8\%\ \ get\ \ sysyem\ intensive\ monitoring\ by\ vendor \\ \geq 8\%\ \ System\ will\ \ temporalily\ paused\ till\ next\ authenticity \end{cases}$$

Case 1: $\boldsymbol{p_a} < 4\%$

$\lambda = np_\text{h}$

$$\equiv \frac{e^{-\lambda} \times \lambda^m}{m!} < 0.04$$

$$\equiv e^{-\lambda} \times \lambda^m < \ \ 0.04 \times m!$$

$$\equiv \frac{\lambda^m}{(m!)} < (0.04) \ \times \ e^{\lambda} \ \text{....................................(5)}$$

Case 2: $4\% \leq \boldsymbol{p_a} < 8\%$

$$\equiv (0.04) \ \times \ e^{\lambda} \leq \frac{\lambda^m}{(m!)} < (0.08) \ \times \ e^{\lambda} \text{....................(6)}$$

The equ^n (5) and (6) shows that the number of blocks (applicants data) that can be attacked by the attacker is entirely depended upon the number of a block generated at that interval. The generation of blocks (applications) is not under the control of the validation administrator. Therefore a validation algorithm is required to control 'm' in the system.

C. Proposed Algorithm for validation

The algorithm of ToSSecC is the mail server to send the email to the corresponding email of the corresponding applicant of the admission system. This primary assumption of the algorithm is that the odd numbers of (three in this case) are considered and at least two out of three must validate honestly. In the first phase of the algorithm, the email id of the applicant is validated by three validator nodes of the blockchain selected by the validator leader and the validator generate an encrypted security key to validate the exact email id of the applicant so that the proper email is sent to the applicant to restrict the spam email.

The security mechanism is mainly important to control the attacker to access the mail server so that the entire admission process would not collapse.

Each node of the blockchain has a public key(pub.ky) and a private key (pvt.ky).

The validator leader (VL) select the three validator node from the by sending K1 to all the nodes

K_1= hash(validator.pub.ky+number)

The validator sends the k2 mail-server(ms) to send the details to the validator.

K_2= hash(K_1, mailserver.pub.key)

The mail server returns the k3 to the validators.

K_3= hash(K_2,mail-server.pvt.key, email to send ackn)

The validators returned the key k4 and validation value true or false in the form of probability($\text{p} = \frac{1}{3}$) to the validator leader,

K_4= hash(validator.pvt.ky+number, K_3),Probability

It is expected in a true case of internal attack at least two validators would respond honestly. If the probability $\text{p} \geq \frac{2}{3}$ then only the validator leader permits the mail-server to send the email to the desired address.

Input:*thepub.key of nodes $\in$ $blockchain\ nodelist$*
Outputs: *True/false, probability p (initially $p = 0$)*

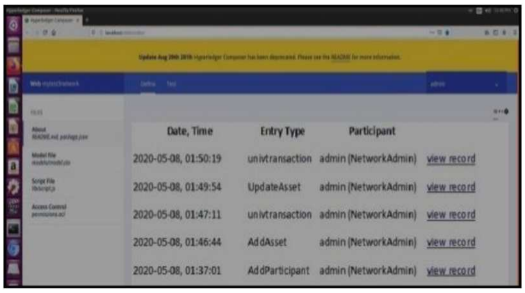
```
1.  for i=1 to i=3   // selection of 3 validator nodes
2.    Send $K_1$ to nodes$\in$ $blockchain\ nodelist$
3.   if encoded pub.ky of node matches with $K_1$ then
4.  VList ⟵ $v_i$   // validator nodes assigned to validator list V
5.  end of if in no. 3.
6.  ms ⟵ $v_i$. $K_2$  // $K_2$ is assigned in ms
7.      $v_i$ ⟵ ms. $K_3$  // $K_3$ is assigned in $v_i$
8.      if (ms. $K_3$ is exist)
9.        value=true
10. $p = p + \frac{1}{3}$  // probability is increased if the value is true
11. Validation Leader ⟵ ms. $K_4$ // $K_4$ encrypted key is returned
12. Validation Leader ⟵ p // Probability is returned to VL
13. else
```

```
14.          value=false
15.  $p = p - \frac{1}{3}$ // *probability is decremented if value is false*
16.   Validation Leader ⟵ ms. $K_4$ // *$K_4$ encrypted key is returned*
17.  Validation Leader ⟵ $p$ // *Probability is returned to VL*
18.       End of if in no. 8.
19.  end of for in no. 1.
20.   if ($p \geq \frac{2}{3}$) // *Probability is $\geq \frac{2}{3}$ then mail server is allowed to email*
21.  ms⟵ permitted to send the email
22.  end of if in no. 20.
23.  end
```

D. Simulation Result

The experimental domain of smart contract is used in Linux 16.4 version and the Hyper Ledger Composer Playground is used to design the smart contract between the university and the students.

In the definition of smart contract, the course-wise admission criteria are defined as the asset (class course). The university and applicable students are defied as participants (class university and class applicants). The result of the incorporation of smart contracts using hyper ledger is shown in figure 5.



Date, Time	Entry Type	Participant	
2020-05-08, 01:50:19	univtransaction	admin (NetworkAdmin)	view record
2020-05-08, 01:49:54	UpdateAsset	admin (NetworkAdmin)	view record
2020-05-08, 01:47:11	univtransaction	admin (NetworkAdmin)	view record
2020-05-08, 01:46:44	AddAsset	admin (NetworkAdmin)	view record
2020-05-08, 01:37:01	AddParticipant	admin (NetworkAdmin)	view record

Fig. 5. Transactions in Hyperledger

Figure 6 shows the expected number of attacking blocks (applicant) to restrict to achieve less than 4% and less than 8% attack, with the generation blocks from 10 to 100 with the interval of 10 generating blocks.

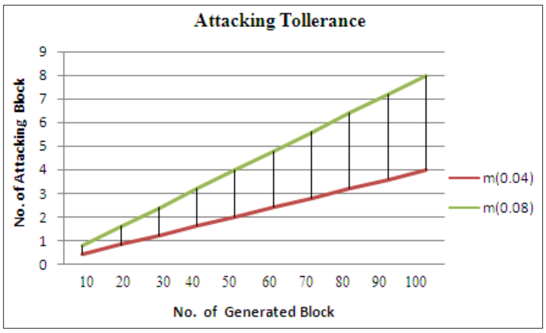


Fig. 6. Tolerance Limit of Attacking Node

The probability of an honest and attacking validator is shown in figure 6. The picture indicates that the threshold probability of an attack of the number of blocks attacked is increased with the increase of the number of generations of the block. The differences in the number of attacked nodes are increased between two cases in equation (5) and (6) respectively (< 4% SPAM attack and < 8% SPAM attack) with the increase of the number of generation nodes.

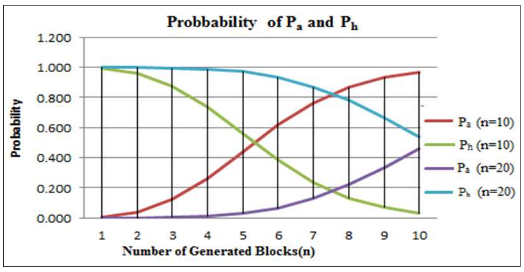


Fig. 7. Probability of Attack and Nonattack

The probability of an honest and attacking state of both the honest user and the attacker is shown in Figure 7. The picture shows that the curve of the probability of attack and honest activities is just the opposite.

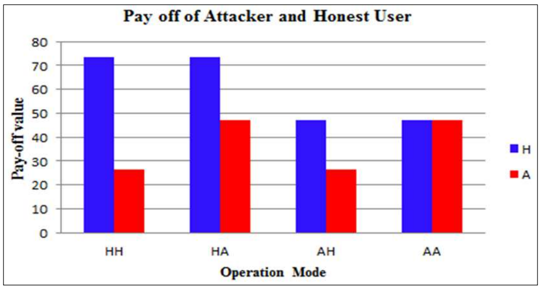


Fig. 8. Pay-Off of Attack and Nonattack

Figure 8 shows the pay-off as described in Table II. In this particular case, some arbitrary values have been taken that H=100, n=10, m=3 P_a=0.265, and P_h=0.735. The value of pay-off of an honest node is much higher when the attacker does not attack. The Nash equilibrium indicates when both the honest and dishonest users attack each other.

E. Discussion and Analysis

In case of the first condition (p_a<4% attack), figure-6 shows that the system will be unaffected from the attack if the number of generated blocks in the system is less than 25, then the system will be free from attack as the number of attacking block is less than 1.

In case of the second condition (p_a<8% attack), figure-6 shows that that the system will be unaffected from the attack if the number of generated blocks in the system is within 10, then the system will be free from attack as the number of attacking block is less than 1.

If the number of nodes is generated in higher numbers, then the probability of chances of suspension of the system is decreased as the tolerance limit of affected nodes is increased (up to a certain value) as shown in figure-6.

In both the cases (p_a<4% and p_a<8% attack), the probability (figure-7) of both the honest node and the attacker are equal (p_a=p_h=0.5) at the time of half of the expected node of generation.

The nonattacking pay-off of the honest nodes is always best. The attacking (increase of security, firewall cost) pay-off of the honest user will be decreased. The proactive defensive measure of the honest nodes also needs to be taken to smoothly run the system with the minimum attacking effect.

V. Conclusion

In this paper, the analysis of different security aspects of clouds has been done. Some of the real situations of security, vulnerabilities of attack of the mail server in the cloud are also considered. The implementation of blockchain, smart contracts in practices proposed in this paper to secure the data. Further, an algorithm is also proposed to validate the generated block before sending any email. These would protect the blockchain from other kinds of vulnerabilities and DDoS attacks. The entire solution is proposed from the perspective of Game Theory. We have also analyzed and have shown the simulated result of the blockchain applications of university admission systems in the domains of the Hyperleder framework.

In the future, there is a plan to explore our research work to address the double-spending attack issues of smart contracts using game theory in the cloud environment. The plan is also to evaluate the cost and complexity analysis of enhancing the security features of cloud data using smart contracts as well in blockchain framework.

References

[1] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends” , IEEE 6th International Congress on Big Data, pp. 557–564, DOI: 10.1109/BigDataCongress.2017.85, 2017.

[2] P. Asuquo, C. Ogah, W. Hathal, S. Bao, “Blockchain Meets Cybersecurity: Security, Privacy, Challenges, and Opportunity”, In: Kim S., Deka G. (eds) Advanced Applications of Blockchain Technology. Studies in Big Data, vol 60, pp. 115-127, DOI: https://doi.org/10.1007/978-981-13-8775-3_5, 2020.

[3] K. Prabhakar, K. Dutta, R. Jain, M. Sharma and S. K. Khatri, "Securing Virtual Machines on Cloud through Game Theory Approach," *2019 Amity International Conference on Artificial Intelligence (AICAI)*, pp. 859-863, DOI: 10.1109/ AICAI. 2019. 8701229, 2019.

[4] Park, Jin H., and Jong H. Park, "Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions", *Symmetry* 9, no. 8: 164. DOI: https://doi.org/10.3390/sym9080164, 2017.

[5] R. Wang, J. He, C. Liu, Q. Li, W. Tsai and E. Deng, "A Privacy-Aware PKI System Based on Permissioned Blockchains," 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), pp. 928-931, DOI: 10.1109/ ICSESS. 2018. 8663738, 2018.

[6] H. Zhou, C. de Laat and Z. Zhao, "Trustworthy Cloud Service Level Agreement Enforcement with Blockchain Based Smart Contract," 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp. 255-260, DOI: 10.1109/CloudCom2018.2018.00057, 2018

[7] R. Tonelli, M. I. Lunesu, A. Pinna, D. Taibi and M. Marchesi, "Implementing a Microservices System with Blockchain Smart Contracts," *2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pp. 22-31, DOI: 10.1109/IWBOSE.2019.8666520, 2019.

[8] R. Jathanna and D. Jagli, "Cloud Computing and Security Issues", International Journal of Engineering Research and Application, vol.7, Issue. 6, DOI: 10.9790/9622-0706053138, 2017.

[9] Z. Xu, F. Li, M. Tan, and J. Zhang, “A Blockchain-Based Distributed Authentication and Dynamic Group Key Agreement Protocol”, in Blockchain and Trustworthy Systems. BlockSys 2020, Z. Z., D. HN., F. X., and C. B., Eds., vol. 1267. pp. 142–151, DOI: 4835; https://doi.org/10.3390/s20174835, 2020.

[10] S. Kim, "Two-Phase Cooperative Bargaining Game Approach for Shard-Based Blockchain Consensus Scheme," in IEEE Access, vol. 7, pp. 127772-127780, 2019, DOI: 10.1109/ ACCESS. 2019. 2939778, 2019.

[11] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar and M. Abdelhag, "Mobile Cloud Computing: Challenges and Future Research Directions," 2017 10th International Conference on Developments in eSystems Engineering (DeSE), pp. 62-67, DOI: 10.1109/DeSE.2017.21, 2017.

[12] Al-Janabi S. Al-Shourbaji I. (2016). A study of cyber security awareness in educational environment in the middle east.Journal of Information & Knowledge Management, Vol. 15, No. 1, 1650007, DOI: 10.1142/S0219649216500076, 2016.