Research Article

Block Chain Technology in Supply Chain Management Using Key Generation

Priti Lale[1], Manish Sharma[2]

[1,2]Deparment of Computer Science & Engineering, Suresh Gyan Vihar University Jaipur, (RJ) India
priti.met@gmail.com[1], manish.sharma@mygyanvihar.com[2]

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27 January 2021; Published online: 05 April 2021

Abstract: An information system is very important in today's changing world, and therefore choosing the proper system is becoming a very important decision. With the time, the information systems have become more crucial, with multiple problems affecting the supply chain and the continuous writing of performance areas. The principle of chain management aims at chain values. The working of chain management states that chain management enhances the value of the chain by establishing operational units. Traditional manufacturing supply chains bear a lot from additional, costs, delays and information loss due to information middleware's. Therefore, we propose a blockchain oriented supply chain architecture to reduce intrusion in traditional ones. Current approaches to private-key security include signature schemes based on bio-metrics, index-hidden private key design, and post-quantum block chain schemes. Nevertheless, recovering the lost private key is difficult in all approaches. Here we proposed an optimal key formation procedure using a fitness-based self-adaptive sea lion algorithm for secure information sharing in SCM using block chain.

Keywords: Supply chain management, Blockchain Technology, Optimization

1. Introduction

Information sharing is the main part behind the supply chain. Blockchain is a attractive IOT technology that can provide many lucrative applications compromises of logistics and supply chains. Recently, the chance of implementing blockchain technology is a lucrative technology in many industries. Blockchain is taking a role from important multiple disciplines, such as medical services, army and other centralized credible identity intermediator (Jian Weng, Ming Lee, Lin Hou, Anija Wang, Jia-Nan Liu, Yang Xiang, Wei Lu, Yue Zhang Robert H. Deng 2018). Blockchain is able to provide an immutable leader solution for many distributed stakeholders by distributed design architecture having heterogeneous designs and technologies which are computationally strong as well as advance. Blockchain security is maintain by verifying the transaction using cryptography of public and private key, and blocks. But the recording of transaction cannot be done. Once modified because they are connected to each other as a part of table they are accepted (Avinash Samvedi, Vipul Jain, F. T. S. Chan, S. H. Chung 2016, Maozhu Jin, Hua Zhang, Yucheng Zeng 2018). There is a block attached at every level which needs to be hidden from the middlemen. Now days, supply chains nature is becoming complex in design, working is difficult, and variety of stakeholders, and large application areas mostly don't have an abstract version of the chain, largely organizations have their Identity created and has the power to instruct systems and their suppliers to manage global coverage of operations. A blockchain oriented supply chain largely recommended and should be reliable in authentication and traceability, eliminating intermediator auditors (Scott DuHadway, Steven Carnovale, Benjamin Hazen 2017). By adopting blockchain technology in SCM, operations management is secured, more transparent, permeable and efficient blockchain technology is liable to increase collaboration among SCM members, thereby indirectly impacting efficiency and cost in the supply chain. Also blockchain technology is able to increase customers' trust, due to the goods traceability throughout their communication between the supply chains (Amit Karamchandani, Samir K. Srivastava, Rajiv K. Srivastavam 2017).

2. Literature Review

The blockchain was first introduced by Satoshi Nakamoto for solving the security problem in electronic transactions. A blockchain is an shared, open and distributed bookkeeping that enables information security and responsibility, and is apt for dealing with important information (Petri Helo, A. H. M. Shamsuzzoha 2020, Xin Wen, Sai-Ho Chung, Xuting Sun, Tsan-Ming Choi 2019). Blockchain technology enables tracking of real-time business communication and synchronization of crucial update documentation, there are multiple problems, such as efficiency, block size, security, scalability and privacy which still require concrete technical solutions. Blockchain has potential applications in various fields, such as medicine records management, SCM, and financial services, liability and accountability management in Internet of Things (IoT), shared and distributed access control (YiHe Liu, Shuang Zhang 2020, Sánchez Sotano, Alejandro J. Magdalena Ramirez-Peña ,Víctor Pérez-Fernandez, Francisco J. Moises Batista 2019).

However, supply chain management has several important issues in its current business operations. First, supply chain management mostly influenced by the enhancing applications of Internet of Things (IoT). Using IoT, the exact locations of packages, containers and products will be easily tracked at every level for achieving transparency in information with supply chain (Shuchih Ernest Chang, Yi-Chian Chen, Ming-Fang Lu 2019). Blockchain technology give users feasibility of recording transactions, but cannot simply be considered as "records", as it has different other features, such as preventing fraud and responding to technical disruptions Smart contract to deliver. Blockchain is basically associated with different technology that enables cryptocurrency, like bitcoin, but, by explaining the idea of blockchain technology with its different applications.

The blockchain technology has features such as decentering, distributed storage, traceability, non-tamper capacity, and smart contracts (Petri Helo, Yuqiuge Hao 2019). Due to the nature of distributed storage one has to go to the center first. Each node of a P2P network always have backup of data for entire blockchain system, and node failure has no impact on the whole network operation. In a blockchain network data storage is permanent, and for tracking information of transmission path timestamp technology can be used. The design of the blockchain restricts it from data tempering (Raja Masadeh, Basel A. Mahafzah and Ahmad Sharieh 2019). The execution situations are programmed by code which is scripted and the execution constraints of the contract are executed automatically when the constraints are met (Geeta S. Navale, Suresh N. Mali 2018, M M Annie Alphonsa, N. Mohana Sundaram 2019).

There are different types of block chains that are in use. Public Blockchain: There is absolutely no restriction on a public blockchain. Simply with an Internet connection it becomes a verifier as soon as they make a transaction. Private Blockchain: A private blockchain is allowed. No one can join unless network administrators send an invitation. Consortium Blockchain: A consortium blockchain is frequently called as semidecentralized. Butin place of a single organization handling it; many companies can operate one node on each such network (Geeta S. Navale, Suresh N. Mali 2018, M. M. Annie Alphonsa, P. Amudhavalli 2018).

3. Proposed privacy preservation using key generation

In this paper a new privacy preservation technique is proposed where by using the process of data sanitization and restoration sensitive information is hidden from the intermediate level which is more vulnerable to the stakeholders involve in communication.

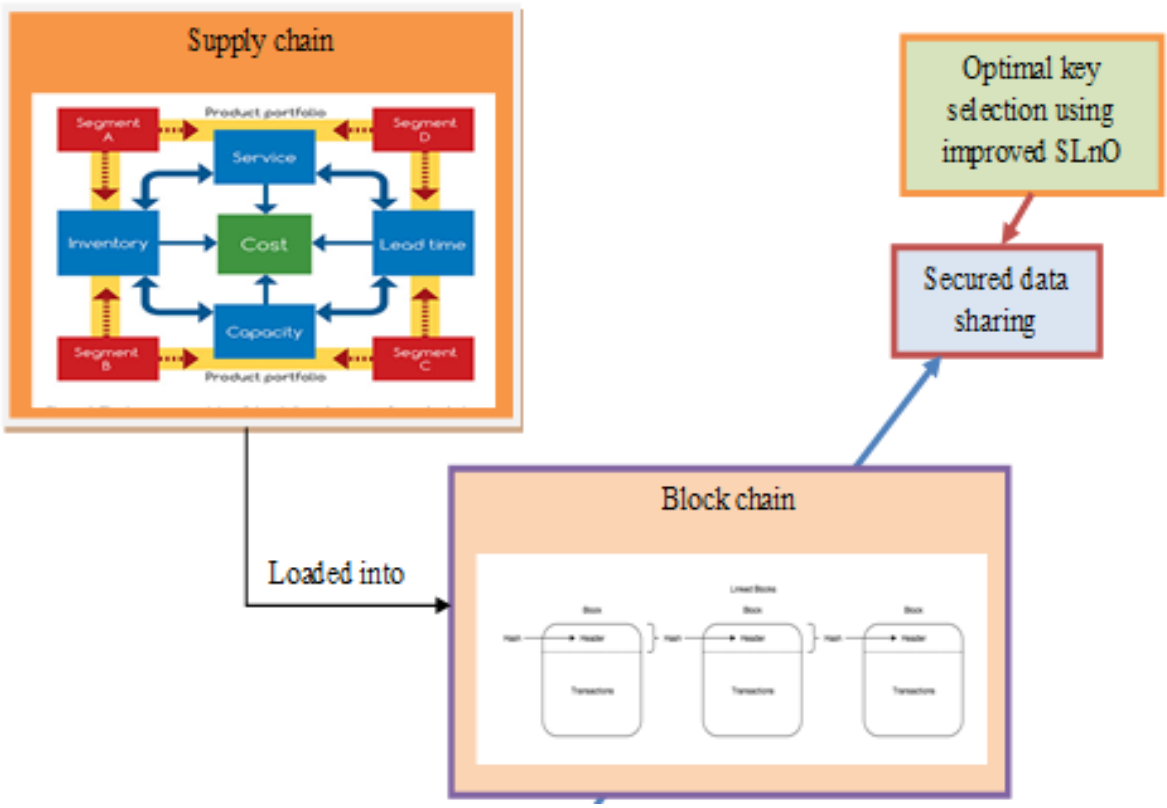

Figure 1. Process of key generation

In supply chain management the data travels from level 1 to level n which is manufacturer to manufacturer and the secure block chain technology is used when processing this data. Manufacturers build their databases with separate fields where there is both a sensitive and a sensitive information, sensitive information needs to be hidden from the manager and the distribution agent. The authentication process takes place at the manufacturer level where, after successful key generation, the key can be passed. The next level by adding data blocks to the block chain (Priti Lale, Dr. Manish Sharma 2020).

Figure 1 shows the services provided in the supply chain where cost, capacity is the major part of the inventory chain. This information is passed on the block chain in which sensitive information is hidden in the block. To make the data secure the optimal key is selected using the optimized fittest self-adaptive sea lion algorithm.

3.1 FSA-SLnO algorithm Mathematical Model

In the mathematical models encircling, tracking and identification of pray attack is explained.

1) Tracking and detecting phase

For representing distance between the target prey and the sea the symbol used is $\overrightarrow{Dis}$, and the vector position $\vec{S}(t)$ and target prey $\vec{M}(t)$ is responsible for position update. For representation of iteration the term t is used and for random vector $\vec{G}$ residing in the interval [0,1] is multiple by 2 for search space enhancement for acquiring optimal solution. The subsequent iteration is represented as $(t+1)$ and here the value of $\vec{H}$ is lessened in a gradual manner from 2 to 0 over the course of iterations.

$$\overrightarrow{Dis} = \left| 2\vec{G}.\vec{M}(t) - \vec{S}(t) \right| \tag{1}$$

$$\vec{S}(t+1) = \vec{M}(t) - \overrightarrow{Dis}.\vec{H} \tag{2}$$

2) Attacking phase

The sea lions in this exploration phase have to locate the target prey and surround them. The “Dwindling encircling technique and Circle updating position” are used to model the prey attacking concept in an effective way.

3) Searching for prey

The sea lions positions update isfor identification of the optimal search agent. In exploration phase, by random selection of sea lion the position of sea lion is updated. Means, when value is greater than one, SLnO algorithm will globally identify search agent and optimal solution will be identified which is again global.

Step 1: Initialization of overall population and assigning index.
Step 2: Finding the fitness of overall population.
Step 3: If ($\overrightarrow{SP_{leader}}$ <0.25)
If $abs(1) < 1$
For $t = idx(1) : idx(5)$ i.e. the first five best solutions of the fitness Fit is updated using the Phase-1 Prey detection and tracking.
Step 4: In case if $abs(1) >= 1$, then update the position of the solution using the exploration phase.
Step 5: Further, if ($\overrightarrow{SP_{leader}}$ >= 0.25), then update the position of solution (first five solutions) using the exploitation of the standard SLnO.

Algorithm 1. Pseudocode of the proposed FSA-SLnO model
Initialization of overall population (Pop) and index (idx)
Find the fitness (Fit) of the overall population
If ($\overrightarrow{SP_{leader}}$ <0.25)
If $abs(1) < 1$
For $t = idx(1) : idx(5)$
The solution update with Prey detection and tracking phase.
Else
the solution with the exploration phase.
Else
For $t = idx(6) : idx(10)$
the solution update with the new update
End
Terminate

4. Conclusion

In this work, the key used will be optimally selected via a up to the minute optimization model referred to FSA-SLnO, The major benefit relied on this process were: Only the authenticated person will be able to retrieve the data shared the sender having same key. The validation of proposed key generation in SCM with block chain technology will be done with comparison with existed model while comparing security as well.

References

1. Amit Karamchandani, Samir K. Srivastava, Rajiv K. Srivastavam (2017). Perception-based model for analyzing the impact of enterprise blockchain adoption on SCM in the Indian service.
2. Avinash Samvedi, Vipul Jain, F. T. S. Chan, S. H. Chung (2016). Information system selection for a supply chain based on current trends: the BRIGS approach. *Neural Comput&Applic*.
3. Geeta S. Navale, Suresh N. Mali (2018). A multi-analysis on privacy preservation of association rules using hybridized approach. *Evolutionary Intelligence*.
4. Geeta S. Navale, Suresh N. Mali (2018). Lossless and robust privacy preservation of association rules in dat sanitization. *Cluster Computing*.
5. Jian Weng, Ming Lee, Lin Hou, Anija Wang, Jia-Nan Liu, Yang Xiang, Wei Lu, Yue Zhang Robert H. Deng (2018). *CrowdBC:* A Blockchain-based Decentralized Framework for Crowdsourcing. *IEEE Transactions on Parallel and Distributed Systems.*
6. M M Annie Alphonsa, N. Mohana Sundaram (2019). A reformed grasshopper optimization with genetic principle for securing medical data. *Journal of Information Security and Applications, Vol.47, pp.410-420*.
7. M. M. Annie Alphonsa, P. Amudhavalli (2018). Genetically modified glowworm swarm optimization based privacy preservation in cloud computing for healthcare sector. *Evolutionary Intelligence*.
8. Maozhu Jin, Hua Zhang, Yucheng Zeng (2018). Supply chain optimization based on chain management mand mass customization. *Information Systems and e-Business Management*.
9. Petri Helo, A. H. M. Shamsuzzoha (2020). Real-time supply chain—A blockchain architecture for project deliveries. *Robotics and Computer-Integrated Manufacturing*.
10. Petri Helo, Yuqiuge Hao (2019). Blockchains in operations and supply chains: A model and reference implementation. *Computers & Industrial Engineering, Vol.136, pp242-251*.
11. Priti Lale, Dr. Manish Sharma (2020). Secured Information Sharing using Data Sanitization and restoration. *International Journal of Advanced Trends in Computer Science and Engineering*.
12. Raja Masadeh, Basel A. Mahafzah and Ahmad Sharieh (2019). Sea Lion Optimization Algorithm. *International Journal of Advanced Computer Science and Applications (IJACSA), vol. 10, no.5*.
13. Sánchez Sotano, Alejandro J. Magdalena Ramirez-Peña, Víctor Pérez-Fernandez, Francisco J. Moises Batista (2019). Achieving a sustainable shipbuilding supply chain under I4.0 perspective. *Journal of Cleaner Production, in communication*.
14. Scott DuHadway, Steven Carnovale, Benjamin Hazen (2017). Understanding risk management for intentional supply chain disruptions: risk detection, risk mitigation, and risk recovery. *Ann Oper Res*.

15. Shuchih Ernest Chang, Yi-Chian Chen, Ming-Fang Lu (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change, vol.144, pp.1-11*.
16. Xin Wen, Sai-Ho Chung, Xuting Sun, Tsan-Ming Choi (2019). The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. *Logistics and Transportation Review, Transportation Research Part E: Vol.127, pp.178-191*.
17. Yi He Liu, Shuang Zhang, (2020). Information security and storage of Internet of Things based on block chains. *Future Generation Computer Systems, Vol.106, pp.296-3030*.