Indian Journal of Science and Technology, Vol 12(23), DOI: 10.17485/ijst/2019/v12i23/145374, June 2019
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Study on Strengthening Privacy and Cyber Security using Block Chain

R. Anusha*, B. Prashanthi, Rupa Rani and Lavanya

Computer Science and Engineering, St. Peter's Engineering College, Maisammaguda, Hyderabad – 500043, Telengana, India; amanuknr@gmail.com, prasanthi.bayyarapu@gmail.com, rupathatipalli111@gmail.com, lavanyagolipally@gmail.com

Abstract

Objectives: The work is to analyze the block chain technology to improve the privacy and cyber Security. **Methods/ Statistical Analysis**: The blockchain can be used in cloud to protect data stored in them and also block chain-based identity and access management system address the key challenges visage in IoT security. **Findings:** The findings show that the blockchain lends itself well to Internet of Things (IoT) applications. It provides more security in the exponentially growing networks and holds each part involved accountable in transaction. Finally conclude that the combination of block chain and IoT can provide a powerful approach which can significantly pave the way for new business models and distributed applications. **Application/Improvements:** The blockchain achieves safety and secrecy of distinctiveness and other private data in health care industry.

Keywords: Blockchain, Cyber Security and Health Care Industry, Internet of Things (IoT)

1. Introduction

The blockchain is an open distributed ledger which allows to record transaction between two teams in an efficient and permanent manner. It allows implanting the contracts in digital format, storing them in shared and transparent database. In this digital world each transaction, process, task payment etc. will have a digital record which can be verified, stored and shared. This is the important feature of blockchain which prevents data from deletion, tampering etc. The blockchain technology can offer sturdy privacy and cyber security protection. The records are stored on many organized computers with identical information[1]. There is no 3rd party involved in storing information. The requirement of more than 1 key improves the security and privacy. As block chain is distributed around many computers, successful hacking requires hacking more than half the systems in the network.

The security approach followed today is to keep the implementation and mechanisms a secret. But the system may breakdown if somebody finds out the structure[2]. The Society for Worldwide Interbank

Financial Telecommunications (SWIFT) is a secure messaging system used by financial institutions. In 2016, a bank in Bangladesh lost more than $ 81 million due to illegal transactions that were directed through the New York Federal Reserve Bank using the SWIFT network. The convention of blockchain-based systems possibly helps in avoiding such attacks. The chance of single point of catastrophe or weakness in blockchain is nil. The most famous application of blockchain - the bitcoin transactions was never compromised, even though attacks were on the systems that hold and store bitcoin private keys.

Now checking the privacy issues, the cyber-attacks are on the legally collected consumer's data which are again used by secondary users illegally. Also, the usage of cloud services may give rise to confidentiality and safety issues. In a blockchain model, there is no obligation to hoard material with third parties who can give rise to confidentiality and safety issues[3]. The private data can be accessed

*Author for correspondence

with the authorization of the subject and the data cannot be warehoused. Also, the identity proof being stored in a cryptographic format, it is very hard to crack them.

2. Security and Privacy Considerations of Blockchain and Cloud Computing

The data kept in the cloud data centers was about 65% in 2015 and will grow to 88% of the total data center storage capacity by 2020. The blockchain and cloud computing handles safety and

confidentiality issues in similar manner. They provide cost-efficient security solutions.

The organizations have to decide on the public and private cloud services. Public clouds are preferred by an organization dealing with more transaction/less-security or low data value while private cloud is suitable for applications that has substantial risk from material exposure such as monetary institutions, health-professional or federal agency.

To meet safety, secrecy and other requirements, two types of blockchains are used - permission less and permissioned chains. Permission less blockchain is open as in bitcoin. Anyone can join. Permission block chains are limiting[4]. Entree must be fixed by some authority. Example of supply chain blockchain is developed by IBM and the Danish shipping company Maersk.

Both the cloud and blockchain are providing high safety protection. They achieve this by various encryption methods. The Cloud Services Providers (CSPs) also follow "zero trust" model for security. Here reliability needs to be measured for every solo device. If an instrument is lacerated, it does not pose risk to the entire network as a user has entree only to particular things. To get access in the whole network, the invaders must outbreak into multiple devices at once. This enhanced model is called as "security micro-segmentation" which is implemented by google. Some CSPs also perform continual examination for distrustful activities and offers real time response to create a cyber reliable zone.

A blockchain is a distributed ledger network using public-key cryptography to cryptographically signed communications that are stored on a distributed ledger, with the ledger containing of

cryptographically connected blocks of transactions. As it is based on cryptography, the data is kept private while transmitting and storing. As blockchain is a latest technology, erudite safety mechanisms do not exist for some systems. Thus, some attacks were on few digital currencies. On an average there are 15-50 defects on software code. As they are not widely used, they are not seriously tested. The design of blockchain may also turn vulnerable as all the systems in the network run the same code. If any hacker detects that vulnerability, then the whole system will face severe consequences[5].

As one of the major downsides of cloud computing is about safety and confidentiality, the cost related to these outweighs the benefits. Also, there is hidden cost associated with security breaches. These drawbacks can be minimized using block chains as shown in Table 1.

3. Blockchain in Health Care Industry

Let's see in brief how blockchain achieves safety and secrecy of distinctiveness and other private data. Basically, there are 3 parties in identity document exchange[6]. 1. Subject of identity, 2. Certifier who may be a government firm and 3. An inquisitor who make an enquiry on the subject. The blockchain has 2 ledgers - accountant ledger and a transaction ledger. The content ledger holds the separately encrypted documents while the transaction ledger holds the encryption key document folder which holds the attributes of the subject. The certifier with the permission of subject puts the digitally certified certificates for various attributes. The examiner may review the document when the subject gives regulated access to keys. All the enquiries are documented for the subject. The third parties may get entree by smart-contract framework. Thus, data stored in blockchain will get higher degree of authenticity.

Health care plays a major role in using blockchain to avail security and privacy services. In non-blockchain model, 3 methods-push, pull and view methodology are implemented to achieve interoperability[7]. In push model, the therapeutic statistics is sent from a provider to another (e.g. from casualty to doctor). In pull model, the data is directed from one provider to another. The view model, the provider checks out another provider's record. In these methods data is not audited properly, hence data integrity may not be maintained from the location of data origination to the data use.

Blockchain allows sharing of health records safely across benefactors during the life span of a patient.

Table 1. An evaluation of the security and privacy provided by cloud and blockchain

	Cloud	Blockchain
Making Efficient and cost effective	Require computers, more software and employ more IT individuals	Eliminates the necessity for third parties in dealings by making a distributed record which is dominated and confirmed by other users.
Implementation	Private, public and community	Permission less and permission chains to meet safety, confidentiality. Certain members are allotted as regulators and auditors
Reinforce cybersecurity	The data is encrypted; Creates a "cyber risk-free zone": continuous tracking for mistrustful actions and real time retorts	The data is completely encrypted Use of Cryptographic hash functions. Public-private key cryptography ensures that the figures is reaching only the prearranged addressee
Challenges	Various cloud benefactors depend on firewall mode to monitor the incoming and outgoing traffic. Criminals may break such systems	This being new technology, it is not widely used and tested.

Blockchain in Electronic Healthcare Records (EHR) avoids including an organization between the patients and the data records. Block chain's time-stamped and programmable ledger permits smart management of record entree. It is not necessary to produce custom realism for every EHR vender. The ledger includes high level audit path. The changes made to the data by consumer are communicated to the public record.

Several public-private enterprises have come up to use blockchain in medical field. MedRec is a decentralized report management system to handle EHRs. It was developed by MIT Media Lab and Beth Israel Deaconess Medical Centre. It manages secrecy, verification, data sharing and accountability. Patients will get access to their medical statistics across various providers and medical care sites. An incontrovertible log of all dealings concerning a patient is created and provided to them. It stores the reports sign on a blockchain which guarantees the readiness of an intact copy to the users. Here the patient decides who can access the data.

Despite these facilities, there are many barriers to move to blockchain. It must address the concerns related to privacy, authentication security etc. Also, the mindset of the healthcare providers must change as they consider themselves as only steward the data given to that organization.

4. Blockchain and IOT

Blockchain and IoT will form a powerful combination which can transform many industries. Combining blockchain with Artificial intelligence, Big Data, better results can be produced.

IoT security has been a keen topic of interest. In 2015 US based security systems Veracode have verified the security of few IoT systems. They found that major security issues within the front end and back end. They didn't use strong passwords and encryption for connections making them defenseless against man in the middle and replay attack. Transport layer encryption was also not implemented making the certificates invalid.

Another attack was on Dyn a U.S.-based Domain Name System (DNS) provider. The attack was with many IoT devices like webcams, video recorders, routers etc. It was attacked with distributed denial of service attack. This involved phishing e-mails to infected computer which then spread to other devices connected to internet used by shops and traders for surveillance. By getting access to these devices the criminals can track the presence and absence of residents are away from home etc.

Severe consequences can occur if IoT devices are compromised. Blockchain is promising to tackle these problems. It can provide military level security for IoT systems. Incorporating blockchain in IoT improves security a lot.

Blockchain promotes faith in the supply chain by making transparent and distinguishability when stocks transfer from the source to client. IBM is taking advantage of its vast cloud framework to offer blockchain services by following top-value items as they move transversely the supply chains.

It permits users to feature elite IoT information to a non-public blockchain registers, which is bounded in shared transactions. The platform recognizes the material from connected devices and convert into the arrangement that blockchain supports. When the products are moved from source to customer, blockchain helps in providing transparency in the supply chain application. This is implemented by Provenance. IBM allows to augment IoT data to confidential blockchain ledgers and in turn to share transactions. An API decodes the data from those devices into that of blockchain. The partners of the contract can ingress and stream IoT data and authenticate the transactions. Only the partners involved in that transaction can access and verify them.

Another application is filament taps which creates autonomous mesh network. Each node depends on the network and mesh nodes permitting the circulation of data. This is used in irrigation and mining operations. The role of blockchains in device identification and intercommunication. It holds the unique identity for each participating node[8].

This can be used in industrial network technology. The devices are connected to sensors, which communicate securely, exchange value among them and implement actions automatically. For instance, a drilling rig identifies the requirement of machinery on which it sends request message to an automated drone. This drone can then get the required machine to complete the operation[9].

Cisco, Bosch, Foxconn Technology, blockchain startups Consensus Systems etc. together designed a group to set an innovative regulation for safeguarding IoT applications using blockchain. They plan to develop blockchain etiquette as a civic platform to build IoT gadget, utility and networks. They formed an API that ropes technologies available like Ethereum-based blockchain systems developed by JP Morgan's Quorum and the Linux-led Hyperledger project. This project allows the user to bind the weaker entities like serial numbers, QR codes to stronger cryptographic entities. These entities are absolute across physical and digital world.

IoT security can be improved by the use of blockchain based identity and access management systems. Once the actual information is entered accurately, then blockchain is immutable. By producing private cryptographic hashes of separate device firmware, everlasting record of machine configuration can be created. This hash can be checked to see if the device is genuine, whether its software is tampered etc. Only after this the device is allowed to adhere to other devices. This feature of blockchain will be accustomed defend against IP spoofing attacks.

All these attacks are based on the centralized cloud model. The risk increases as the nodes grows making it difficult to manage and expensive[10]. Thus Decentralized, block chain-based approach will be more effective for upcoming IoT systems. Let's discuss the various challenges faced by centralized IoT system[11]. As the existing IoT solutions are growing on a large scale, network capacity must also be increased in that scale. This will increase the cost exponentially. Large server granges and networking machines are needed which upsurges the setup and preservation costs.

Most IoT equipment direct information into the cloud and communications will be sent from the cloud to the devices[12]. This poses a security threat to IoT. There can be bottle neck and can act as point of failure making it susceptible to DDoS attacks, data thefts, hackings, and remote hijackings[13]. If an IoT device connected to server is lacerated, then all devices connected in that network can be attacked[14].

In the long run, blockchain can eliminate many of the above draw backs. It allows secure data exchange between nodes in the system. Blockchain can sign the transaction cryptographically and also verifies the signature ensuring that the message is sent by the accurate originator. This can in turn prevent man in middle attack and replay attacks.

5. Conclusion

As seen in the discussion above, blockchain may prove hazardous for cyber criminals, data manipulators etc. Blockchain will be a promising approach to deal several features of security and privacy issues. It allows the individuals to secure their personal data.

Many challenges faced in cloud can be dealt with autonomous, decentralized properties of blockchain. It provides more security in the exponentially growing networks. It holds each part involved accountable in transaction. Most of the hacking activities can be reduced to great extent by implementing cryptographic security. It enables costless verification of attributes of participating device. IoT security threats associated with IP spoofing can be handled by blockchain-based identity and access management systems.

6. References

1. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy. 2017; 41(1):1027–38. https://doi.org/10.1016/j.telpol.2017.09.003
2. CTO Corner: What is a blockchain and why is it important? FS Roundtable; 2016.
3. How blockchain improves security and transaction times. Nasdaq. 2917. https://due.com/blog/blockchain-improves-security-transaction-times/
4. A public or private blockchain? New Ethereum project could mean both. 2017. https://www.americanbanker.com/opinion/a-public-or-private-blockchain-new-ethereum-project-could-mean-both
5. Blockchain's weak spots pose a hidden danger to users. 2017. https://www.technologyreview.com/s/604219/blockchains-weak-spots-pose-a-hidden-danger-to-users/
6. Google adopts zero trust network model for its own cloud. 2019. https://techcrunch.com/2019/04/10/google-cloud-unveils-new-identity-tools-based-on-zero-trust-framework/
7. The Internet of Things poses cybersecurity risk. 2017. https://www.itproportal.com/features/the-internet-of-things-the-cyber-security-risks-and-how-to-protect-against-them/
8. A secure model of IoT with blockchain. 2017. https://www.slideshare.net/altoros/a-secure-model-of-iot-using-blockchain
9. IoT and blockchain Convergence: Benefits and challenges. 2018. https://www.researchgate.net/publication/325486515_Blockchain_with_Internet_of_Things_Benefits_Challenges_and_Future_Directions
10. Blockchain and Cloud kissing cousins. 2017. https://www.digitalistmag.com/digital-economy/2017/04/26/blockchain-cloud-kissing-cousins-05043776
11. Hacked home devices caused massive Internet outage. 2016. https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/
12. Companies forge cooperative to explore blockchain-based IoT security. 2017. https://www.ciodive.com/news/companies-forge-cooperative-to-explore-blockchain-based-iot-security/435007/
13. Researchers show that IoT devices are not designed with security in mind. 2015. https://www.pcworld.com/article/2906952/researchers-show-that-iot-devices-are-not-designed-with-security-in-mind.html
14. Blockchain could help fix IoT security after DDoS attack. 2016. https://venturebeat.com/2016/10/29/blockchain-could-help-fix-iot-security-after-ddos-attack/
15. How blockchain can change the future of IoT. Venture Beat. 2016. https://venturebeat.com/2016/11/20/how-blockchain-can-change-the-future-of-iot/