A Survey on Blockchain Security System and Proactive Integrity Proofing Model in Centralized Cloud Environment

Dr. R. RENUGA DEVI[1]

K. GANGADEVI[2]

[*1] Assistant Professor, Department of Computer Science and Applications (MCA), SRM Institute of Science and Technology, Ramapuram, Chennai
drrrenugadevi86@gmail.com
[2] Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, India
deviganga1979@gmail.com

Abstract

Blockchain technology impact of security is a huge development on many businesses based on secured information processing, transactions, and safety to make in communication, and it still affects many places, due to what it can do for privacy levels. Although the characteristics of blockchain technology make security services in a centralized cloud environment, But most of the innovative technology doesn't provide standards security levels from service management. The development of blockchain leads to more security based on cryptographic issues. The exploration focuses on recent development challenges in the Blockchain security system and then summarizes the specific security threats. We consider some ideas in potential research directions based on security improvements. In this review, K. Hao et al, describe the explore integrity proofing using cryptographic security related to Blockchain model technology and its application. With supportive factors consider destroying many technical areas in the future, deals with security factors. However, it will be upgraded in areas that have been discouraged from many new security areas. Security concerns, not only from some unexpected areas but also from distributed/distributed computing issues and information encryption algorithm issues. The resultant of these conventional algorithms produce a different level of terms of analysis that are reviewed on the rest of the sections.

Keywords: cryptography, blockchain security, integrity proofing, information security, cloud computing.

1. Introduction

Cloud computing provides various services that are based on the pay scale to use methods to access different services. The author S. Nepal, S. Chen et al. described that cloud services are provided by Cloud service providers (CSP) based on the application, infrastructure, and platform network technologies. The issue of cloud computing security is so important that cloud computing, especially integrity calibration, can prevent using the differential problem consideration to improve security. Sustainability, Cloud Computing Systems, and Analysis Fixed computing users and

owners perform policy. Cloud policy, security issues, storage, network, and security according to software limited network computing cloud services. (SDN) are services that are provided on a cloud-based basis such as services. Services are provided to these types of users.

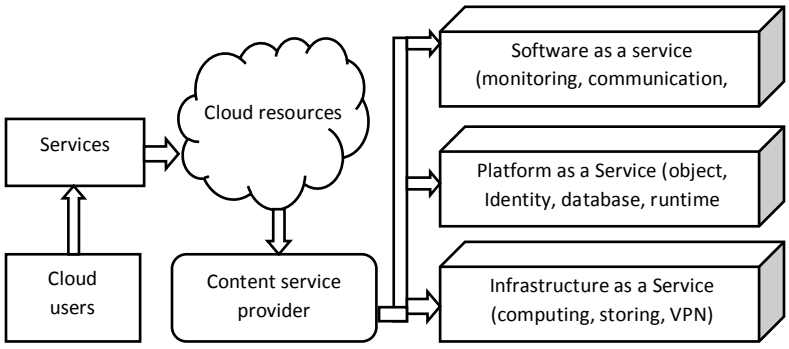

Figure 1: Process of cloud computing

The cloud environment maintains different data elements in different systems. Various data accessing cloud resources provided by cloud service providers. So due to all the service providers due to various concerns companies are helping to reduce the maintenance costs of their data. Because cloud storage (Kun Hao et al) is a remote task that requires them access to a variety of data and services, cloud storage data is always accessible anywhere, anytime.

In addition to this, it is leading and rising like another worldview to navigate services on the Internet through storage services provided by cloud providers, registered assets across servers and applications. Figure 1 shows the Process of cloud computing depends on the partition the cloud integrity management will be a reliable cloud of calculations based on storage, security, broadcast security, virtualized computing security, and system calibration key verification will not know. From Dang et al reference, Hardened public and private clouds are required at various levels to provide end-user protection. Then, another variable called the Service Level Agreement (SLA) that obscures the provider's shared liability between users.

2. Cloud and its Security Standards

Utilizes information concealment and key matching technology Centralized security here recognizes security standards and public cloud services. By the reference author Park et al, Encryption in some coded form of the owner's policy, security proof tetchiness based on the use of different encryption algorithms. Data protection and decryption Oppose encryption to protect data. The decryption ciphertext converts the original text to the default R using the decryption algorithm with the representation key provided by the correct person. Traditional cryptocurrencies are also the symmetric cryptocurrency and security proof optimized algorithms for cloud protection, DSAs are called RSA and then DES, AES. Security generally refers to three main aspects: reliability,

integrity, and availability. Also, the cloud model must meet the requirements of authentication, access control, privacy, trust, audit, and compliance.

Confidentiality: Term Privacy refers only to the authorized individual or entity that has access to the information and power of protected information. The cloud will increase as compromises on devices and services increase due to data confidentiality. Multi-rental giant, infrastructure reuse, virtualized multiple privacy, and confidentiality threats present. Data confidentiality can be separated due to careless data recall. But the rest of the existing data after the data should be erased or deleted.

Integrity: In general, view resources, data, hardware, and software in the cloud. User data is geographically separated clouds, and the stored data will undoubtedly be processed by cloud providers cloud users because ASIL (atomicity, stability, independence, and life) are then properties. Beneficiaries of Cloud Providers (Service Level Agreements) must change the accuracy and reliability of the data supported and ensure certain technical compatibility. Cloud consumers should provide mechanisms such as audit, disaster recovery, data backup, incident response, and integrity proofing to confirm the safety.

Privacy: Privacy is a personal option to disclose certain confidential information. Companies must comply with national legal frameworks in dealing with sensitive information of individuals. Cloud announced the existence of data servers around the world due to many legal and privacy challenges in forecasting. The fact that these legal rules and compliance varies from country to country. Cloud providers want to see what high transparency and exposure is for its cloud users. Cloud customers should be provided with appropriate security mechanisms to protect sensitive information. Trusts are used to enable customers to be convinced that the system itself is secure and accurate. In a cloud environment, the cloud will provide a variety of services for completely dependent cloud users. To use these services, the user submits confidential data to the provider. Thus, it is necessary to capture a general set of metrics in establishing the competent confidence to develop a framework of trust

These issues complicate authentication and access control issues and introduce multiple vulnerabilities and threats. Therefore, ensuring the reliability and completeness of the stored data is the most challenging issue in the cloud compared to traditional models. The following are the security threats facing companies in the adoption space of the cloud computing model.

- Data theft– Unauthorized individuals steal sensitive information. Compromise certificates, laws, broken credentials such as passwords, fingerprints, etc. stolen user credentials

- Insecure APIs-Risk Access to users via insecure APIs can be increased during CSP. Malicious virtual machines running under the same hypervisor and all other virtual machines as a virtual machine-malicious in the attack.

- Data Wipe-Data Representation of the rest of the data to gain knowledge of important data. Permanent data loss-data can be destroyed due to Byzantine failure or data that is rarely accessed can be ignored. Less diligence increases the risk when cloud users do not fully understand the

environment and the risks associated with it. Abuse of cloud services- Misuse of cloud services for launching attacks like DoS (Denial-Of-Service)attacks, phishing, etc.,

- Service Attack Denial is charged for decoration services or data not available. It is important to mitigate these security threats in the cloud and impose security requirements on cloud data and services.

3. Concept of Blockchain and characteristics

Blockchain Technology by Qin and Zhao et al point of reference, the Concept blockchain is a one-of-a-kind technology that includes encryption, mathematics, protocols, and economic models defined by Barinov et al. It also integrates peer-to-peer networks to security concern on distributed problems. It is integrated using a distributed consensus algorithm to solve multi-sector infrastructure construction. Blockchain technology consists of the main components. A blockchain system typically displays a block, a hash of sensitive data, a hash of the previous module, the current module have the reaction id to correlate the block. The timestamp holds the representation of access data on the related block. This Blockchain application works through the key hash code. After they have cleaned the code they make transmissions.

- Blockchain uses the Merkel tree function to generate a random hash code on each block with a decision tree structure to relate the block because it cannot contain thousands of transaction logs for blocks on each node. It can use the Merck tree function to spread data to significantly reduce forecast resources, and the time stamp finalizes the key code to verify the transaction security. The following are the characteristic of Blockchain security
- Observation and monitoring. Data, which records data through the Blockchain system, is obvious why Blockchain is trustworthy. Open source integrity. Most Blockchain systems logs are stored as centralized to access with verified integrity from access policy control to use with an aggregated owner policy
- Autonomy. Based on a consensus, the idea is that one person throughout the system is in the form of trust and that each node in the Blockchain system can be securely replaced or because the data update is interfering with everyone. Immutable. All achievements are forever set aside and cannot be changed until other users validate the access control provider to the requested user.
- Anonymous. Blockchain technology solves the problem of trusting relationships between nodes that only the person knows the Blockchain address should be noted because data transfer or transaction can be anonymous.

4. Working Principle of blockchain

Node New Data, Network Sending Details Cast) 1 login: The key labor steps in the blockchain are as follows. 2) If the message is correct, the node receives confirmation that after receiving the message from this data, it is stored in the block. 3) The network was also found to have all receiving knots to execute work (transaction) proof or stock-proof (POS) mechanisms.

A) Consensus This functionality is a mechanism that allows Blockchain to agree on the same message with all nodes to ensure that the latest module can be generated to be added to the chain exactly, indicating that the node is saved as well. There are no guarantees that "war attacks" have taken place, but still protects against malicious attacks.

B) **Proof of Work (PoW)** Job proof is hard to create (expensive or time-consuming) but subject to some requirements met by others. The task of creating the task can be a random process, knowing that the majority of the investigation requires an average of error before proper evidence is generated. By changing this untested value, the blocks are randomized and grouped with order value and this block title has a hash value that is already set to harder rather than the transaction. Most of the verification are authenticated by block network participants by Third Party Auditing (TPA), the mining block must cover all of the data and complete proof of work. This block is set to reduce the rate at which any new modules network can create difficulty every minute. The successful generation has a very low probability, which is unpredictable because it can create the next batch of workers computers in the network

C) Proof of Stake (PoS) Steak Proof is not a creative method Waste is the source of many sources of electrical power, does not require expensive computing skills. Evidence and Comparative Resources of Stocks Bitcoin miners can hold the amount less percentage considers the Bitcoin mines owned by someone who can verify the integrity proofing. The following are the responses from proof aviated to verify the consensus. Specifically, Bitcoin refers to the near majority with the non-supportive authentication with reduction state need more block verification to suffer leads chances to attackers. The continuous execution refers to the verification authenticity links refers to a consensus algorithm, by every node on network verifies the transaction information with the block of the state.

5. Reviews and related works

The following are the various author described by various methods of block verification. **Hao Wanga et al described the** cloud storage services. But at that time, the program suffers from a lot of potential problems. **Dongdong yue1 and ruixuan li et al described** verification methods that can lead to completely false verification results to reduce computational overhead in block-based programs. However, this mechanism is not supported by data entry. **Wang et al**. addressed this issue. Supports effective PTP mechanism and functionality will be fully dynamic. Table 1: Comparisons of blockchain methods and their limitations

Author/Year	Tittle/Transaction	Techniques Used	Limitations/Drawbacks
P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar,2020	Blockchain data-based cloud data integrity protection mechanism/ Future Generation Computer Systems.	Multi-tenant model, virtual agent verification	Ensuring participation in all communications, data, and audit policies major leaks and security systems failures.

Y. Zhang, C. Xu, X. Lin, and X. S. Shen, 2019.	Block chain-based public integrity verification for cloud storage against procrastinating auditors," IEEE on Cloud Computing,	Public key crypto policy, TPA, certificate less public verification scheme	This technique eliminates the expensive process of mapping authentication whereas it pop-ups an essential need to share the common lookup chart amongst
K. Hao, J. Xin, Z. Wang, and G. Wang, 2020	Outsourced data integrity verification based on blockchain ," World Wide Web,	collaborative Verification Peers (VP's), verification group (VG) policy	The main problem with asymmetric encryption is the enormous amount of computation and storage required. Encryption failure to decade security.
R. Kalis and A. Belloum, 2018	Validating data integrity with blockchain, IEEE Cloud Computing Technology, and Science (CloudCom).	Data identifier and a hash technique, blockchain-based hash validation	The lack of secure connections but public data hackers already exchanged with devices for theft and attack.
S. Wang, D. Zhang, and Y. Zhang, 2019.	Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable, IEEE Access,	fine-grained access control, searchable symmetric encryption.	Malicious users can easily discuss and plan illegal activities to bring instant TPA auditing systems leads more time
D. Yue, R. Li, Y. Zhang, W. Tian, and C. Peng, 2018:	Blockchain-based data integrity verification in P2P cloud storage, (ICPADS)	Traditional verification framework involves the Third Party Auditors (TPAs)	It also makes it easier for major leaks to plot illegal activities as they discuss it with malicious users.
D. Kraft, 2016	Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications	exponential hash, Poisson process with time-dependent intensity	Key leakage problem arise security has already been applied to nonintegrated security in many areas and unsecured views.
Y. Zhu, H. Hu, G.-J. Ahn, and S. S. Yau, 2012	Efficient audit service outsourcing for data integrity in clouds," Journal of Systems and Software,	Provable data possession (PDP), Diffie–Hellman assumption.	The quality problem of traditional random lighting types is used to improve system security.

Although the Provable Data Partition (PDP) authentication mechanism can effectively check data integrity, it cannot recover invalid data. The problem with incomplete trusting is that traditional data integrity verification must use Internet Blockchain technology to integrate Blockchain technology for cloud storage data integrity verification (population) is an inevitable trend. This framework can provide more reliable verification of data tonnage, data ownership, and data consumer data integrity regardless. However, their work is targeted at the top of the population and does not apply to P2P cloud storage displays. **Yuan Zhang et al defend the process of blockchain,** General Verification Technology defends the public integrity proofing the check the authentication by using the TPA principle. The initiates usually verify the proofing authentication of data, and if a check fails to report, the user has corrupt data. In most public verification programs, auditors are considered honest and reliable. These plans will not work if the auditor is at risk. For example, a reckless auditor can always create a good integrity statement without the fantastic reception of verification costs to avoid. The auditor, like one of those, is almost there.

Nurzhan zhumabekuly aitzhan et al described the Blockchain resource is the forward chain of time-series sequence of protected blocks resolving work. Besides, the blockchain integrates storage verification and the current level of permission with the previous volume hash to the next volume current volume hash. Chronologically coming and subsequent built-in modules are guaranteed transactions, so a transaction module cannot change its backdate without changing all the modules below. A centralized network is an important component, providing targets for availability, reliability, and security, as full authentication and payment activities are intercepted and intercepted as centralized intermediary nodes fail. **Rosco Kalis et al** describes the functionalities of Data users from different application domains to ensure that they do not take the data incorrectly and corruption. Check the integrity of the data, not to mention a Blockchain-based hash verification method. Electronic Audit Tracks (EDT) and other data that already exist decades ago and ensure data integrity with other data on demand. These immoralities as audit trails can be added in some overcoming ways and made worse in a variety of ways. Then, at the end of the century how many other tasks to preserve audit record data on unreliable computers were then first cited concerning data integrity and audit. It uses a comparable method to create review test data supplementary secure regularly database.

Huaqun wang et al explained the secure storage of remote data Cloud computing is very important. All existing Peer to Peer (PTP) verifies programs utilize RSA or two-line integration. A large file must be divided into large volumes.

Dejia wang et al implemented the secure cloud storage Achieving large population data integrity verification efficiently and Things Internet has a security policy to verify the integrity proofing on cryptographic applications. Reliable Third-Party Auditors (TPAs) rely on cloud-protected data encryption technology with traditional data integrity verification methods. Blockchain-based data integration programs can thwart confidence issues with successful TPAs, but they also face significant computational and communication overhead issues. **Ning Lua et al defined as** the best of our community become more interconnected, more data (population) tools

will be stored as remotely as things available on the Internet. These devices and services are usually operated on privately owned external sources (e.g., commercial cloud servers). Therefore, this was interested in using a program involving a third-party auditor (TPA) company to verify the completeness of such transmitted data, be in virtualized server storage be verified to allow the security by integrity proofing levels. But the existing solution is relevant to blockchain integrity proofing leads more time complexity.

Kun hao et al described the As an important service provided by cloud service providers (CSPs), data outsourcing can effectively enable the data owner Denial of Service (DOS) to deal with large-scale storage vulnerabilities of data. To solve the problem, Blockchain's innovative landscape models were used, including distributed architecture, unnecessary storage, bulk maintenance, and fraud protection. To report the key issue, we will make copies of the data store in a blockchain-based outsourcing service in unreliable environments, including the first three main layers: storage layer, validation layer, and blockchain layer. After that, the validation in Virtual Private Security (VPS) invented a new concept to maintain the meta stored in blockchain format, to prevent the meta from being corrupted by each of them. Grab the entire Blockchain locally. **Jianfeng Ma et al described the** cloud storage system offers users with a suitable data storage service that allows for outsourced data access and updates remotely. Therefore, a general audit is required and an integrity audit of data sent by a Third Party Auditor (TPA) company is required. Many public audit systems are highly involved in data and communication resources and are considering the limit 'Users use public audit programs to audit the completeness of their outsourced data. These prevailing audit conventions are primarily based on the Access Control Systems (ACS). However, Indonesian communist-based auditing systems pose key management issues.

6. Potential aspects and cryptographic failures in the blockchain

Some security issues and other issues with blockchain processes (author Kiayias et al) generally prevent all individuals from controlling the basic infrastructure in our thread review programs that it distributes many protocols and adheres to the same protocol that focuses on blockchains running peer-to-peer networks. Blockchain relies on the security, strength, and stability of the encryption resources used to maintain a comprehensive history of past operations to carry out transactions. Based on asymmetric key encryption called Digital Signature Algorithm (DSA), information encryption hashes are the main algorithm used in Blockchain implementations. Based on Algorithm Blockchain technology has always been the choice of application developers.

Blockchain Trust relationship: Blockchain does not force colleagues to have a trusting relationship between them. However, Blockchain does expose the data reliability between the security service makes trust relation suing blockchain.

Consensus troubleshooting: Troubles begins from attacks which can repeat the un-authentication access through the attacks happen, for example, Initialize the security Blockchains Bitcoin only the consensus troubleshooting and fast-declaring blocks that have been declared illegal, can rest easy

by accepting more power than half of the hashes over block control, where they and all the fellow attackers are enduring.

Vulnerability contracting: Blockchain smart contracts will focus more on transparency and transparency. Every error that exists is completely known all the authenticators, this is because all the member nations, it embraces attackers begins to block.

6.1 Problematic resources and services factors

Block chain resources are filtered by the enemy with the help of a collective attack.

Fraud in Programming: Thief attack can be used for internal programming encryption such as Blockchain natural exploitation scam. **Private Key leakage:** Attackers retain with frequent to access the account to theft the key. **Circular point of encrypted attacks**: By the non-authentication encryption, key leakage problems depend on the traversal node according to the circulate attacks by peers points at point eclipse traverse node region.

7. Blockchain security and integrity proofing on cloud

Blockchain is a powerful computing technology that distributes to the cloud, implementing validation security and management processes. The author Amine Ferrag et al define IoT Blockchains can be used by customers to integrate distribution networks to operate secure information sharing, secure data management, supply chain management, service of food suppliers and retailers. The Black Chain is a separate interconnected, Customer Contact Certification System (CCCS) called Secure Management (SM)

A) Blockchain security

The only key used is to encrypt and delete. Public Key Encryption (PKE) is called symmetric cryptography or public-key encryption. Separate keys are used for encryption and decryption. Contains algorithms and keys in the process of systematization. The key text is not related to a specific value. Different products depending on the specific key used at the time of the procedure. Changing the key changes the algorithm output. Once Cypher text is created, it can be sent to cloud storage. The received Cypher text will not be converted to the original default using the decryption algorithm with the same key used for encryption.

B) Blockchain integrity proof

The primary purpose of the blockchain chain was to assist without the help of TPA assistance to verify the authentication in access to decentralized security (Ben-Sasson et al). Using this technology all users of the system can access the network data. The problem is conflicts in these characteristics in the Privacy Law Foundation (PLF). These laws require a party to handle personal data on behalf of the individual to provide data protection and privacy.

This is a control of the database from shared peer-to-peer network deals as well as sharing. It is an array of connected modules that, over time, can hold Public-Key Encryption (PKE), and

conduct transactions verified by the network community. This manages a series of computers (Timestamp) of non-interactive data records. Each of these data blocks surrounded by encryption has a similar size. Categorization is public and private access control security. Private blockchain chains are prohibited instabilities of admittance, where it is very significant to decrease the number of multiple contributions not by the entire network of user collisions. Most of the connections are associated and supplementary if any other of these within the module is verified by TPA. The trade parade already blocks it with a timestamp and a hash link attached. Cryptography produces a realistic amount of transactions with Advanced Encryption Standard (AES). All over the key management verifies the security improvement by compete to create new modules. Adding to the public ledger is the total transaction cost, but is delivered only to the actual block generation, as well as to the main minors.

8. Security developments in Blockchain Cryptography

Blockchain concentrated from above issues with security integrity proofing all over the key management verifies the security improvement by compete to create new modules. Adding to the public ledger is the total transaction cost, but is delivered only to the actual block generation, as well as to the main access with TPA key management. Blockchain, who held a key position in digital encryption technology. Protection of manipulator evidence and data transfer is a fundamental disorder for Blockchain development.

8.1 Security services use Blockchains and issues

Facilitate resource tracking process without the need for a blockchain distribution, fitting, and registration of centralized trust companies makes issues on security companion. Where it is distributed to both parties and decisions are made by the majority Peer-To-Peer Network, allowing communication and currency resources instead of a single centralized authorization. They essential to produce that cancellation management, distribution, utility infrastructure, and store keys and information. Global Treasurer, Blockchain Technology The role of the Blockchain network is so common to all nodes that it can receive a complete copy of the store transaction description. Attacks can occur that threaten the user's transactional privacy and identity privacy. The transaction privacy threat mechanism allows the attacker to capture transaction records and explore valuable information.

8.2 Blockchain-based privacy-Awareness Authentication

Blockchain technology failed compared to traditional encryption technology and the user shunned. There are many benefits to having faith to solve a problem at one point. Blockchain technology creates a Privacy Sense Authentication Program for a multi-server environment in which a shared registry and efficient cancellation can be realized. Also, the program not only provides multiple security requirements such as mutual assurance, username, and full-forward secret but also does not resist various malicious attacks. At the boot stage, build user registration,

user cancel, and re-registration is done carefully. The program may be subject to security and privacy threats during the certification phase.

8.3 Security-Enhanced Network Coding by Public-Key Cryptography

Security coding can only be achieved through a Linear Networking coding (LNC) vector network connection when there are a certain number of attacks, and security is otherwise not guaranteed. In the most realistic scenario where it is connected to any number of eavesdropping attacks, using LNC based security and asymmetric key encryption technologies to provide data protection.

8.4 Hierarchal cryptography security in WSN

Secure communication is a big problem in cryptographic improvements algorithms like RSA, DSA, DES, AES and makes power controls from TPA, the composite may be suitable for secured trust transmission in Wireless Sensor Networks (WSN) that control many key security mechanisms. Key maintenance on WSN is a multifaceted assignment because of its restricted nature. The hierarchical data transmission network sensor node holds the secretly shares the panel key. Getting started is key to sharing malicious intruders or terminals on a password-protected network. Introduction to defensive threat technical analysis.

8.5 Security algorithm using hybrid cryptography

Due to address the increasingly serious problems, Security attacks such as authorization, authentication, integrity, non-refundable, availability, and security services to various symmetric and asymmetric encryption methods are created with a combination of symmetrical and asymmetric encryption strategies. Encrypt sources of honesty, reliability, and authenticity.

8.6 White box encryption based data encryption-decryption program

To provide security, data encryption is an unavoidable condition, and symmetric algorithms are becoming an important implementation in limited environments. Elliptic Curve Cryptographic (ECC), Searchable Encryption (SE) are conventional which are stored as a presumptive express and encryption key security that applies to the communication node. However, the device may be protected, and malicious data stored on it may still be encrypted. It becomes complicated for a malicious person to get this and it is necessary to retain the key. Encryption technology such as white box technology is used in both of these situations. However, it is said that white box access to an average value such as encryption, and code enhancement attacks and duplicate attacks can be used for security issues due to enemies who are executing

8.7 Impact of Security and performance analysis

The data are a secret form of a surreptitious distribution program that can ensure confidentiality at multiple sensor points transactions. When TPA fails on differential condition specifically integrity level of access control, its function may not be restored. The Base Station (BS)

network shares keys between different sensor nodes. Each secret is shared by the key at different sensor points, BS can a few sensor nodes that have failed their secret function or reset the body suffer as long as at least tons due to energy consumption or recovery of the sensors. Unplugged or attacked can always recover keys from all the sensors is the nodes they get key to and even, they are not always able to identify the value of the wireless sensor network. The wireless sensor network maintains selective sharing attacks, Sibyl attacks, Hello flood attacks, pit attacks, spatial hypothetical connection attacks, from privacy security attacks such as the main partitioning mechanism. Confidential sharing program Confirms or blocks an attacker's covert attack on a wireless sensor network. The secret stock of silicon is assigned by BS. Legitimate sensor node BS shared secret cannot be detected by the main network.

9. Conclusion

In these reviews, there are various aspects (theory of enforcement) which are classified into different types of problems and authors can be done to prevent these problems using cryptography integrity proofing methods. The Blockchain will focus on security issues. We point out that the latest Security policies and procedures to improve resistance from cyber-attacks. We will be able to stepup some of the identified vulnerabilities in the reviews and discover some new intergrity proofing vulnerabilities. We have more current novel investigation tendencies in blockchain expertise, to improve the cloud security services, and specifically finance security services often occur in many areas of our lives when blockchain will tremendous as future research to optimize cryptography in multi-objective consideration to improve the security.

References

1. S. Nepal, S. Chen, J. Yao, and D. Thilakanathan, "DIaaS: Data integrity as a service in the cloud," in 2011 IEEE 4th International Conference on Cloud Computing, 2011: IEEE, pp. 308-315
2. Y. Zhang, C. Xu, X. Lin, and X. S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," IEEE Transactions on Cloud Computing, 2019.
3. K. Hao, J. Xin, Z. Wang, and G. Wang, "Outsourced data integrity verification based on blockchain in untrusted environment," World Wide Web, pp. 1-24, 2020.
4. N. Lu, Y. Zhang, W. Shi, S. Kumari, and K.-K. R. Choo, "A secure and scalable data integrity auditing scheme based on hyperledger fabric," Computers & Security, vol. 92, p. 101741, 2020.
5. H. Qin, M. Zhao, X. Wei, H. Shen, and W. Susilo, "Blockchain-based fair payment smart contract for public cloud storage auditing," Information Sciences, vol. 519, pp. 348-362, 2020.
6. R. Kalis and A. Belloum, "Validating data integrity with blockchain," in 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2018: IEEE, pp. 272-277.
7. H. Wang, Q. Wang, and D. He, "Blockchain-Based Private Provable Data Possession," IEEE Transactions on Dependable and Secure Computing, 2019.

8.H. Wang and J. Zhang, "Blockchain-Based Data Integrity Verification for Large-Scale IoT Data," IEEE Access, vol. 7, pp. 164996-165006, 2019.

9. D. Yue, R. Li, Y. Zhang, W. Tian, and C. Peng, "Blockchain based data integrity verification in P2P cloud storage," in 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 2018: IEEE, pp. 561-568.

10. C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meet strong consistency," in Proceedings of the 17th International Conference on Distributed Computing and Networking, 2016, pp. 1-10.

11. Kun Hao , Junchang Xin, Zhiqiong Wang , Keyan Cao , And Guoren Wang , "Block chain-Based Outsourced Storage Schema in Untrusted Environment ", in IEEE access ,pp. 10.1109/ACCESS.2019.2938578, 2019.

12. T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, ''BLOCKBENCH: A framework for analyzing private blockchains,'' in Proc. ACM Int. Conf. Manage. Data, 2017, pp. 1085–1100.

13. H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, ''Towards scaling blockchain systems via sharding,'' in Proc. Int. Conf. Manage. Data, 2019, pp. 123–140.

14. S. Han, Z. Xu, Y. Zeng, and L. Chen, ''Fluid: A blockchain based framework for crowdsourcing,'' in Proc. Int. Conf. Manage. Data, 2019, pp. 1921–1924.

15. J. H. Park and J. H. Park, ''Blockchain security in cloud computing: Use cases, challenges, and solutions,'' Symmetry, vol. 9, no. 8, p. 164, 2017.

16. A. Dorri, S. S. Kanhere, and R. Jurdak, ''Blockchain in Internet of Things: Challenges and solutions,'' 2015, arXiv:1608.05187. [Online]. Available: https://arxiv.org/abs/1608.0518.

17. I. Barinov, V. Lysenko, S. Beloussov, M. Shmulevich, and S. Protasov, "System and method for verifying data integrity using a blockchain network," Patent 2 018 025 181, 2018. [Online]. Available: http: //www.freepatentsonline.com/y2018/0025181.html

18. R. Kalis, "Using blockchain to validate audit trail data in private business applications," Jun. 2018. [Online]. Available: https://esc.fnwi. uva.nl/thesis/centraal/files/f1051832702.pdf

19. A. Kiayias and G. Panagiotakos, "Speed-security tradeoffs in blockchain protocols," IACR Cryptology ePrint Archive, vol. 2015, p. 1019, 2015.

20. Iuon-Chang Lin1,2 and Tzu-Chun Liao2 " A Survey of Blockchain Security Issues and Challenges International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017

21. . Amine Ferrag M, Derdour M, Mukherjee M, Derhab A (2018) Blockchain technologies for the internet of things: research issues and challenges. IEEE, New York

22. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. IACR Cryptology ePrint Archive **2014**, 349 (2014)

23. Li M, Weng J, Yang A, Lu W, Zhang Y, Hou L, Liu J-N, Xiang Y, Deng RH (2017) Crowdbc: a blockchain-based decentralized framework for crowdsourcing. In: Technical report, IACR 444

24. Lin C, He D, Huang X, Choo K-KR, Vasilakos A V (2018) Bsein: a blockchain-based secure mutual authentication with fne-grained access control system for industry 4.0. J Netw Comput Appl 116:42–52.
25. Qin D, Wang C, Jiang Y (2018) Rpchain: a blockchain-based academic social networking service for credible reputation building. In: International conference on blockchain. Springer, New York, pp 183–198