IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 6, June 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006090

Security Mechanism to Prevent Cyber Attack on Cloud Services

Aditi Raina[1], Poonam Bhokare[2], Sakshi Borkar[3]

Bharati Vidyapeeth College of Engineering for Women, Pune, Maharashtra, India

ABSTRACT: Cloud computing is a new environment in computer oriented service. Cloud computing delivers the computing services which includes storage, database and software over the internet. These cloud computing services are easily accessible to all users due to public network. Therefore the security is the biggest issue of this system, because the services of cloud computing is based on the sharing. This project is based on providing security to data, stored over the cloud with the help of blockchain. The data is stored over the cloud is encrypted. The encryption of the data helps in providing secure method of storage of data. The system consist of three modules user, system and attacker. To provide more security to the system authentication is checked. User can put an updating request to the system. If user is authenticated then request is accepted otherwise system block that request and consider him as attacker. The security to the system is provided with the help of blockchain and SHA 256 algorithm. Using public and private secret keys authentication is checked. Hence using blockchain data become more secure and system becomes more powerful.

KEYWORDS- Cyber Attack, Cloud Computing, Block chain, SHA 256 Algorithm.

I. INTRODUCTION

Cloud computing and block chain technology are the two on-demand technologies that are booming within the modern market and are getting used by enterprises
Worldwide. One common difference between the two is that the records of the ledger databases in blockchain technology are immutable, whereas data stored within the cloud is mutable. In this system basically 3module are included i.e. user, system and attacker. To produce more security to the system authentication is checked. User can update data by putting up an updating request to the system. If user is authenticated then updating request is accepted otherwise system block that request and consider that user as an attacker. System provides security with the assistance of blockchain and SHA 256 algorithm. Using public and private keys authentication is checked. Only user and system can view the ultimate data.

Objectives:

- To maintain data security.
- Implementation of SHA 256 algorithm for encryption of data into hash value.
- Block the attacker if he tries to update anything on data.
- Authorized person can access data easily and can modify also.

II. LITERATURE SURVEY

[1] Nurzhan Zhumabekuly Aitzhan et. al. implemented proof-of-concept in decentralized energy trading system using blockchain technology, anonymous encrypted messaging streams and multi-signatures, enabling others to anonymously negotiate the prices of energy and perform trading transactions in a secure manner. Some case studies were conducted to perform security analysis and performance evaluation within the context to invoke security and privacy requirements.

[2] Paula Fraga-Lamas1 et. al.
analyzes the great potential of applying blockchain technologies to the automotive industry highlighting its cyber security features. Thus, the applicability of blockchain is evaluated after examining and evaluating the state-of-the-art

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006090

and inventing current challenges of the main stakeholders. Further, this article describes the use cases which are relevant, since the adoption of blockchain in a broader way and unlocks a wide area of short- and medium-term promising automotive applications that creates new business models and even interrupt the car-sharing economy as we know it. Finally, after studying a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis, some recommendations are listed with the aim of guiding companies and researchers in future cyber resilient automotive industry developments.

[3] Jing Liu et. al. stated major contributions of our survey work come from three aspects. First, after redeeming all-sided research studies, 53 most related papers are selected which shows the state-of-art of the topic, in which 20 papers focus on providing security assurance of blockchain smart contracts, and 33 papers focuses on the verification of correctness of blockchain in the smart contracts. Secondly a taxonomy was proposed towards the topic of security verification of blockchain smart contracts and identify the pros and cons of each category of related studies. Third, through in-depth of analysis of these studies, the correctness of the verification of smart contracts based on the conventional methods which has already become most significant and effective method to validate whether a smart contract is accurate and credible. So, further present representative studies of formal verification of smart contracts in detail to demonstrate by using a conventional method to validate blockchain smart contracts must have a promising and meritorious future.

[4] Freya Sheer Hardwick et. al. proposed a potential new e-voting protocol and e-voting system that utilises the blockchain as a transparent ballot box. The protocol has been designed to stick to the fundamental e-voting properties as well as offer a degree of decentralisation and allow the voter to change or update their vote (in the permissible voting time). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view of application in both development or deployment and usage contexts. Concluding the paper using a blockchain technology is a potential roadmap which is able to support complex applications.

III.EXISTING SYSTEM APPROACH

The proposed CIDS is constructed and deployed on could computing infrastructure because of its heterogeneous model and virtualized technology. Multiple cloud providers exchanges the logs between them for an event and share the data that is altered on malicious software activities amongst themselves. The proposed CIDS is made and deployed on could computing infrastructure due to its heterogeneous model and virtualized technology. Significant researches in Blockchain and intrusion detection to provide security on the data stored in cloud and detect the cyber-attacks which are existing and emerging. The identification of events which are malicious and to provide the privacy to the data is facilitated through learning based model. Such models can even provide additional security and privacy assurances during the live migration of Virtual Machines (VMs) within the cloud and to safeguard Internet of Things (IoT) networks. This might allow the secure transfer of VMs between data centres or cloud providers in real time. The paper proposes Deep Blockchain Framework (DBF) which is designed to present security-based distributed intrusion detection and privacy-based blockchain with smart contracts in the Internet of things networks. The intrusion detection method is utilized by a Bidirectional Long remembering (BiLSTM) deep learning algorithm to house sequential network data and is assessed using the datasets of UNSW-NB15 and BoT-IoT. The privacy based blockchain and smart contract methods are developed using the Ethereum library to produce privacy to the distributed intrusion detection engines.

IV.PROPOSED SYSTEM APPROACH

A blockchain is a chronologically ordered chain of blocks which make the data unaltered and provide transparency. The chaining is done by adding the hash of the previous block to the current block, the hash of the current block to the following block, and so on. Consecutive nested blocks guarantee transactions to return during a chronological order, hence a transaction cannot be changed backdated without changing its block and all the next blocks. The blockchain is controlled by collective voting of unknown nodes, that are honest and adversary nodes participate in generation of blocks. In proposed system blockchain helps to provide security against attacks like modification, reshuffling or deleting of knowledge as attacker isn't able to perform operations, as data is stored in chronological ordered, and if he wants to perform attack then he has to change all the following blocks which isn't possible. SHA-256, or Secure Hash Algorithm 256, is a hashing algorithm accustomed convert text of any length into a fixed-size string of 256 bits. A hash isn't 'encryption' – it cannot be decrypted back to the primary text. It is a 'one-way' cryptographic function.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006090

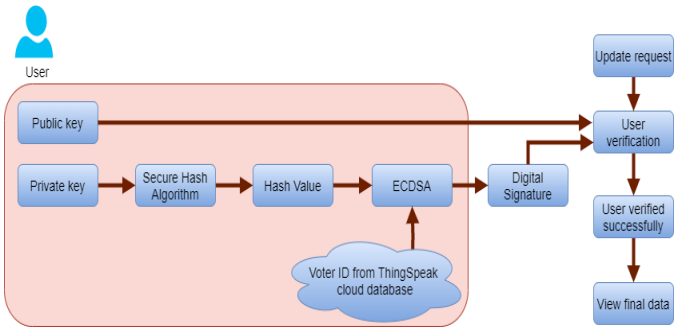

Fig.1 Block Diagram of Proposed System

This makes it suitable when it's appropriate to match 'hashed' versions of texts, as critical decrypting the text to urge the initial version. Digital signatures are rather more involved, but in essence, you will sign the hash of a document by encrypting it with private key, and digital signature is produced for the document. Anyone else can then make sure the person is authenticated by decrypting the signature with the public key to induce the initial hash again, and comparing it with their hash of the text. In proposed system the data that is stored over the cloud is encrypted. The encryption of the information has helped in providing a secure method of storage of data. Because the information is being stored over the cloud, then it'll be accessed by the other authenticated members of the system. During this proposed system user, system and attacker are present. To provide more security to the system authentication is checked with the help of username and password. Admin can login to the system and perform operations on data like upload data of recent user, update the existing user data. If user is authentication is successful then the updating request is accepted by the system otherwise system block to that request and considers that user as an attacker. System provides security with the help of block chain and SHA 256 algorithm. Using public and private secret keys authentication is check. Only user and system can view the final data. In this system if public and private key is matched then only system can updated the record otherwise it will not update. Therefore using blockchain data becomes more secure and system becomes powerful.

METHODOLOGY USED IN PROPOSED SYSTEM:

The data that is stored over the cloud is encrypted. Encrypting the data helps in providing storage of data in a secured manner. As the data is being stored over the cloud, it can be accessed by the other authenticated members of the system. In this proposed system user, system and attacker are present. To provide more security to the system authentication is checked. System can login first, upload the data after authentication. User can update data by putting up an updating request to the system. If user is authenticated then updating request is accepted otherwise system block to that request and considers that user as an attacker. System provides security with the help of block chain and SHA 256 algorithm. Using public and private secret keys authentication is checked. Only user and system can view the final data. In this system if public and private key is matched then only system can update the record otherwise not. Hence using blockchain data becomes more secure and system becomes powerful. Using SHA 256 algorithm hash value is generated for each of parameter of data. The system consist mainly there modules are system, user and attacker viz, User Module, Attacker Module, System Module.

V. CONCLUSION

A cloud is something that we can gain access through the internet. It is a cyberspace which is used to access online data. On the other side, blockchain is said to be an encrypted system that uses different styles of encryption and hash to store data in protected databases. The system distributes these data records over various nodes and forms a consensus on the position of the data they contain. In this proposed system user, system and attacker are present. To provide more security to the system, authentication is checked. If user is authenticated then updating request is accepted otherwise system block to that request and consider that user as an attacker. Using SHA 256 algorithm hash value is generated for each parameter of data. In proposed system using public and private secret keys authentication is checked. Only user and system can view the final data. Public and private key is matched and then system can update the record. Hence using blockchain framework data becomes more secure and system becomes powerful.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 10, Issue 6, June 2021||

DOI:10.15680/IJIRSET.2021.1006090

REFERENCES

1. N. Z. Aitzhan and D. Svetinovic, **"Security and privacy in decentralized energy rading through multi-signatures, blockchain and anonymous messaging streams,"** IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840-852, 2019
2. P. Fraga-Lamas and T. M. Fernández-Caramés, **"A review on blockchain technologies for an advanced and cyber-resilient automotive industry,"** IEEE Access, vol. 7, pp. 17578-17598, 2019.
3. J. Liu and Z. Liu, "**A Survey on Security Verification of Blockchain Smart Contracts,"** IEEE Access, 2019.
4. F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, **"E-Voting with blockchain: an E-Voting protocol with decentralisation and voter privacy,"** in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1561-1567
5. Thite S., Thakore D. (2020) A Survey on the Internet of Things: Applications, Challenges and Opportunities with India Perspective. In: Kumar A., Paprzycki M., Gunjan V. (eds) ICDSMLA 2019. Lecture Notes in Electrical Engineering, vol 601. Springer, Singapore. https://doi.org/10.1007/978-981-15-1420-3_138
6. Sandip Thite, J. Naveenkumar. (2021). FASSSTeR: A Novel Framework Aligned with ISA and ISO Standards for Cyber Physical System Safety, Security, Sustainability and Resiliency. Design Engineering, 2021(02), 399 -411

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details