iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

BLOCKCHAIN-BASED DECENTRALIZED AUTHENTICATION MODEL SCHEME EDGE AD IOT ENVIRONMENT

K. Kuluthan
Assistant Professor, Sri Muthukumaran Institute of Technology, Anna University, Chennai.
S. Nithesh Kumar
Sri Muthukumaran Institute of Technology, Anna University, Chennai.

ABSTRACT
Authentication be the first entrance to kinds of information systems; however, traditional centered single-side authentication be weak ad fragile, which has security be of single-side failure or breakdown caused by outside attacks or internal cheating. In the edge ad IoT environment. blockchain can apply edge devices to better serve the Internet of Things ad provide decentralized high security service solutions. In be paper, we proposed a blockchain-based decentralized authentication modeling scheme (named Block Auth) in edge ad IoT environment to provide a more secure, reliable ad strong fault tolerance novel solution, in which each edge device be regarded as a node to form a blockchain network.
We designed secure registration and authentication strategy, blockchain-based decentralized authentication protocol, ad developed the blockchain consensus, smart contract, ad implemented a whole blockchain-based authentication platform in support of the feasibility, security and performance evaluation. The analysis ad evaluation show that the proposed Block Auth scheme provides a more secure, reliable ad strong fault tolerance decentralized novel authentication with high-level security driven configuration management. The proposed Block Auth scheme be suitable in support of password-based, certificate-based, biotechnology-based, ad token-based authentication in support of high level security requirement system in Edge ad IoT Environment.

Keywords:
Blockchain, Security and privacy issues, Edge and IOT environment, Case *etc*…….

INTRODUCTION

As one of the most important entrances to kinds of information systems, authentication plays a prominent role in information system protection, which ensures the right user have access to the right system with the right identity. Currently, the identity authentication technologies are consist of 1) Password-based authentication. 2) Certificate-based authentication. 3) Biotechnology-based authentication, in support of instance, face, fingerprint or sound recognition. As be known to all, the password-based authentication system stores the hash value of user's password in the database, ad compares the current new password hash values with the stored hash of the original password. If they are consistent, the authentication be passed, otherwise the authentication will be rejected. Although the password-based authentication method be easy to achieve, some serious security problems are existed, such as the brute force cracking ad the dictionary attack. In order to ensure the identity information be not tampered ad destroyed, Certificate-based authentication uses digital certificates in the authentication process, which be regarded as a extremely secure and reliable way.

LITERATURE SURVEY

1.Title: EAC: A Framework of Authentication Property **in support of** the IOTs
Author: Licai Liu; Lihua Yin; Yunchua Guo; Bingxing Fag
ABSTRACT: Authentication be a slick ad importat security property ad its proposed formal definitions are not widely agreed upon. Moreover, these definitions canot faithfully express the requirements of diverse security ad privacy in the Internet of Things (IOTs). To solve these problems, we proposed a framework of authentication, which including three forms of authentication -- entity authentication, action authentication ad claim authentication -- ad formalized each definition by using CSP in support ofIOTs in be paper. We show that the framework ca easily express different security requirements of IOTs ad verify authentication of protocols.

2.Title: Aonymous Secure Framework in Connected Smart Home Environments

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Author: Pardeep Kumar

ABSTRACT: —The smart home be a environment where heterogeneous electronic devices ad appliace are networked together to provide smart services in a ubiquitous maner to the individuals. As the homes become smarter, more complex ad technology dependent, the need in support ofa adequate security mecha the be with minimum individual's intervention be growing. The recent serious security attacks have shown how the Internet enable smart homes ca be turned into very dagerous spots in support ofvarious ill intentions, ad thus lead the privacy concerns in support ofthe individuals. In support ofinstace, a eavesdropper be able to derive the identity of a particular device/appliace via public chanels that ca be used to infer in the life pattern of a individual within the home area network. Be paper proposes a aonymous secure framework (ASF) in connected smart home environments, using solely lightweight operations. The proposed framework in be paper provides efficient authentication ad key agreement, ad enables devices (identity ad data) aonymity ad unlinkability. One-time session key progression regularly renews the session key in support ofthe smart devices ad dilutes the risk of using a compromised session key in the ASF. It is demonstrated that computation complexity of the proposed framework be low as compared with the existing schemes, while security has been significatly improved.

3.Title: A Provably Secure Mobile User Authentication Scheme in support ofBig Data Collection in IoT-Enabled Maritime Intelligent Trasportation System

Author: Khalid Mahmood

ABSTRACT: The emergence of contemporary technologies like cloud computing ad the Internet of Things (IoT) has revolutionized the trends in the cyber world to serve humaity. There are plenty of applications in which they are being used, especially in smart cities ad their constituents, Maritime Trasportation System (MTS) be one of them. The IoT-enabled MTS has the potential to entertain the growing challenges of modern-day ship trasportation. Secure real-time data access from numerous smart IoT devices be the most critical ad crucial exercise in support ofBig Data acquisition in IoT-enabled MTS.

Therefore, we have developed a Physically Unclonable Function (PUF) based authenticated key agreement solution to deal with be challenge. Be solution enables the mobile user ad IoT node to mutually authenticate each other via Cloud-Gateway before real-time data exchage ad trasmission in IoT-enabled MTS. The use of PUF in our solution brings invincibility against physical security threats. A inclusive security aalysis under the assumption of the specified threat model is carried out to substatiate the security resilience of our solution. The conduct of our solution be realized through security features, communication, ad computation cost ad It has been observed that our solution achieves efficiency of 37.3% ad 9.7% in communication ad computation overhead, respectively. Moreover, the network performance effectiveness of our solution be demonstrated in NS3 implementation.

4.Title: Blockchain Meets Edge Computing: A Distributed ad Trusted Authentication System

Author: Shaoyong Guo

ABSTRACT: As the great prevalence of various Internet of Things (IoT) terminals, how to solve the problem of isolated information among different IoT platforms attracts attention from both academia ad industry. It be necessary to establish a trusted access system to achieve secure authentication ad collaborative sharing. Therefore, be article proposes a distributed ad trusted authentication system based on blockchain ad edge computing, aiming to improve authentication efficiency. Meanwhile, a asymmetric cryptography be designed, to prevent connection between nodes ad terminals from being attacked. Ad a caching strategy based on edge computing is proposed to improve hit ratio.

5.Title: A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes

Author: Rada Almadhoun; Maha Kadadha

ABSTRACT: These days, IoT devices are deployed at a massive scale, with Cisco predicting 20 billion devices by the year 2020. As opposed to endpoint devices, IoT devices are resource-constrained devices, incapable of securing ad defending themselves, ad ca be easily hacked ad compromised. Fog computing ca augment such capacity limitations by providing localized compute, storage, ad networking in support of group of IoT devices. As fog nodes are deployed in close proximity to IoT devices, fog computing ca be more effective this cloud computing. Furthermore, Blockchain has emerged as technology with capabilities to provide secure management, authentication ad access to IoT devices ad their data, in decentralized manner with high trust, integrity, ad resiliency. In be paper, we ourselves propose a user authentication scheme using blockhain-enabled fog nodes in which fog nodes interface to Ethereum smart contracts to authenticate users to access IoT devices. The fog nodes are used to provide scalability to the system by relieving the IoT devices from carrying out heavy computation involving tasks related to authentication ad communicating with the blockchain. We ourselves

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

describe system components, architecture and design, we ourselves discuss key aspects related to security analysis, functionality, testing a implementation of the smart contracts. The full code of the smart contracts in support of authentication registry, lists, rules ad logic is also made publicly available at Github.
In is paper, we ourselves propose a user authentication scheme using blockchain-enabled fog nodes in which fog nodes interface to Ethereum smart contracts to authenticate users to access IoT devices. The fog nodes are used to provide scalability to the system by relieving the IoT devices from carrying out heavy computation involving tasks related to authentication communicating with the blockchain. We ourselves describe system components, architecture design, we ourselves discuss key aspects related to security analysis, functionality, testing implementation of the smart contracts.

SYSTEM STUDY

The feasibility of the project be analyzed in be phase ad business proposal be put forth with a very general plan in support of the project ad some cost estimates. During system analysis the feasibility study of the proposed system be to be carried out. Be is to ensure that the proposed system be not a burden to the company. In support of feasibility analysis, some understand of the major requirements in support of the system be essential.
Three key considerations involved in the system studies are

- ECONOMICAL STUDY
- TECHNICAL STUDY
- SOCIAL STUDY

♦ ECONOMICAL STUDY

The study be carried out to check the economic impact that the system will have on the organization. The amount of fund that the company ca pour into the research and development of the system be limited. The expenditures must be justified. Thus, the developed system as well within the budget ad be was achieved because most of the technologies used are freely available. Only the customized products had to purchased.

♦ TECHNICAL STUDY

Be study be carried out to check the technical feasibility, that is, the technical requirements of the system. Ay system developed must not have a high demand on the available technical resources. Be will lead to high demands on the available technical resources. Is will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required in support of implementing be system.

♦ SOCIAL STUDY

The aspect of study be to check the level of acceptance of the system by the user. Be includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead them must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system ad to make him familiar with it. Be level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he be the final user of the system.

Existing System:
Unfortunately, the current traditional authentication methods, such as the ones introduced above, are centralized schemes, which are weak ad single-side with poor fault tolerance and reliability. Meanwhile, they have the following be advantages.
1) The current single authentication has the hidden danger of single point failure, which be easy to be the target of the attacker, because the attacker ca easily for identity ad others to implement the invasion.
2) Blindly trust the authentication agency will bring major security problems, the authentication agency may issue the wrong type of certificate, ad are vulnerable to hacking, forgery, ad falsification of digital certificates.
3) It be difficult in support of a single organizantion to provide multiple types of identity data on which comprehensive multi-factor authentication depends. Moreover, when a single orgnaizantion be attacked, its corresponding local multi-factor identity data ca still be leaked.
In the centralized network, all management rights are gathered in the central node, which bears a huge risk because of the significant responsibility given.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Proposed System & Advantages:

- To protect the privacy, the sensitive data be encrypted before outsourcing. We conduct comprehensive experiments on real-world datasets ad perform comparisons with existing works to evaluate the performance of the proposed schemes.
- The proposed Block Auth scheme has following advantages: collaborative authentication, strong fault tolerance, decentralization, stability ad high-level security.
- In addition, is scheme can meet the authentication requirements of multiple scenarios ad development demand of the international standard authentication scheme.
- High security. It helps to prevent the two cloud servers from inferring each other's sensitive information.
- Data was secure
- By the different fields create a unique block be used to search a user need.

CONCLUSION

In order to solve the security and reliability of traditional authentication in the edge ad IoT environment, we proposed a Block Auth Scheme, which ca provide a more secure, reliable ad strong fault tolerance decentralized novel authentication solution with high-level security. In be scheme, each edge device be regarded as a node to form blockchain network. Specially, we designed the secure registration and authentication strategy and the blockchain-based decentralized authentication protocol, improved the blockchain consensus, developed smart contract, and finally implemented the whole blockchain-based authentication platform in support of the feasibility, security and performance evaluation. According to Evaluations ad Comparison with the existing related scheme, our scheme enhances security and stability on the basis of sacrificing a certain degree of time complexity, ad meets the high security ad fault tolerance requirements of identity authentication in edge ad IoT environment. Furthermore, this scheme proposed by us ca meet the authentication requirements of multiple scenarios ad development demand of the international standard authentication scheme.

REFERENCES

[1] Proc. Roy. Soc. A Math. Phys. Eng. Sci., vol. 426, no. 1871, pp. 233-271, 1989.
[2] M. Abadi ad M. R. Tuttle, "A sematics in support ofa logic of authentication", Proc. 10th Anu. ACM Symp. Princ. Distrib. Comput., pp. 201-216, 1991.
[3] Hung-Yu Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication ad Strong Integrity. IEEE Trasactions on Dependable ad Secure Computing, vol.4, pp.227-340, 2007.
[4] Jia-Lun Tsai ; Nai-Wei Lo. A Privacy-Aware Authentication Scheme in support ofDistributed Mobile Cloud Computing Services. IEEE Systems Journal, vol.9, pp.805-815, 2015.
[5] Muhammad Ajmal Azad; Samira Bag; Charith Perera; Mahmoud Barhamgi; Feng Hao. Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network. IEEE Trasactions on Industrial Informatics, vol.16, pp.3606-3615,2020.
[6] Libor Dostálek. Multi-Factor Authentication Modeling. 2019 9th International Conference on Advaced Computer Information Technologies (ACIT).
[7] K. M. Renuka ; Saru Kumari ; Dongning Zhao ; Li Li. Design of a Secure Password-Based Authentication Scheme in support ofM2M Networks in IoT Enabled Cyber-Physical Systems. IEEE Access, vol.7, pp. 51014 – 51027, 2019.
[8] T.-D. Nguyen, A. Al-Saffar ad E.-N. Huh, "A dynamic id-based authentication scheme", Proc. 6th Int. Conf. Netw. Comput. Adv. Inf. Maage. (NCM), pp. 248-253, Aug. 2010.
[9] S. Chen, M. Ma ad Z. Luo, "A authentication scheme with identity-based cryptography in support ofM2M security in cyber-physical systems", Secur. Commun. Netw., vol. 9, pp. 1146-1157, 2016.
[10] X. Sun, S. Men, C. Zhao ad Z. Zhou, "A security authentication scheme in machine-to-machine home network service", Secur. Commun. Netw., vol. 8, no. 16, pp. 2678-2686, 2015.