International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-10, Issue-4 ,2023 Regular Edition E-ISSN: 2349-7084

ICN Scheme and Proxy re-encryption for Privacy Data Sharing on the Block Chain

M. Prasad [1], K. Durga Sai Divya [2]

[1] *Associate Professor, Computer Science& Engineering at Shri Vishnu Engineering College for Women (Autonomous), Bhimavaram, A.P, India*

[2] *PG Student,Shri Vishnu Engineering College for Women, Bhimavaram, India*

e-mail: drmprasadcse@svecw.edu.in , durgasaidivya@gmail.com

**Corresponding Author: M.Prasad*

https://doi.org/10.22362/ijcert/2023/v10/i04/v10i0405

Received: 01/03/2023, Revised:09/04/2023, Accepted: 18/04/2023 Published:28/04/2023

Abstract:- Data sharing has emerged as one of the most useful applications in cloud computing of the Internet of Things. As interesting this technology is, data security is always a challenge, as improper data use causes a variety of problems. We suggest a ICN Information Centric Networking and proxy re-encryption to protect data sharing in service provider like cloud contexts through this study. Data owners can employ identity-based encryption to send data to the cloud which is encrypted by data owner, while proxy re-encryption allows valid users to access the data. Because the connective devices in IOT have limited resources, an integrated edge devices or edge device works as a server that act as a proxy to conduct demanding calculations . In addition, we leverage ICN characteristics in proxy for distributing cached material efficiently, making excellent use of blockchain and boosting service quality, a revolutionary technology which promotes decentralisation while data exchange. Inefficiencies in centralised systems can be reduced and achieves finely arranged data access management. An alternative to the present Internet architecture, Information-Centric Networking (ICN), mainly concentrates on the distributing the content or the information and retrieval of content rather than the flow of information or content between specified finale stage or endpoints. In the Information centric network, we can see the usage of caches where during high communication traffic network lines mostly the transforming of the data is being avoid from the source to the consumers. Here the copies are placed in on-path in-network caching and this focus is done in this study. Based on the popularity rate of the content or the data, Prob-PD method, calculations of each nodes distance ration, from the result of caching performance, cache's hit rate cache's replacement rate and data delivery times, the study is done. To that end, comparison of simulation results is compared early for the caching approach with existing alternatives, demonstrating considerable algorithm benefits which are proposed.

Keywords: Privacy Enhancing Technologies, Identity-Based Encryption, Information-Centric Networking, Identity-Based Proxy Re-encryption, Internet of Things, Access Control, Caching data

1. Introduction

As an important emerged technology, The Internet of Things (IoT) takes an enormous place in today's world, and over the years its use has resulted in a significant increase in

network congestion volumes. Many gadgets are projected to be connected soon. Data is a crucial concept in the Internet of Things paradigm since the data collected is used for a variety of reasons in applications like healthcare industries, automobile networks, networked smart cities, industries, manufacturing and many. The sensor devices are extremely beneficial to the concerned parties to detect variety of factors. As inviting as Internet of Things is to be, its advancement has presented new issues [6] regarding security and privacy [3][2].

Internet of Things must be secured against attacks which can block its ability to provide essential services, as well as those that threaten data confidentiality, integrity, and privacy. Encrypting data before sending it to cloud servers is a potential approach. When typical security measures [7] fail, encrypted form of data is only appeared to the attackers. To ensure the confidentiality of information or data shared, all information and data at the source should be encrypted and only authorised users can decode [1][3].

Techniques that are utilised here are traditional encryption techniques, where the data owner selects the decryption key and that is shared to all the data users. The usage of symmetric encryption assumes that both data owner and users share the same key, or that the parties agree to have a single key. This solution is ineffective. Now the data owners do not know who the intended data users are, hence the encrypted data must be decrypted and then again encrypted with a key that is known to both the data owner and the data users. This decrypt-and-encrypt system requires the data owner to be always connected to the internet, which is virtually impossible [5].

2. Motivation

Internet of things has advanced as a technology which has enormous relevance over the globe and its use has given leap up to an increased enlargement in network congestion size over the years. In the next year many gadgets and devices are seen to be connected. Data and information are a crucial concept in the Internet of Things paradigm since the data collected serves several objectives in applications or implementations like healthcare industry, automobile networks, new technology-based cities, industries, and manufacturing factories, among others. The sensor devices expose a different type of element that are very beneficial to the parties that are concerned. As a result, as appealing as Internet of Things appears as, its progress has presented new issues related to privacy and security. Internet of things must be secured in opposition to attacks that impede its ability to provide essential services, as well as those that threaten data privacy, data confidentiality, and data integrity [3][5].

3. Existed System

Here we will be modifying the method such that collaboration between the revoked users and service provider is avoided. The plan was to essentially being replaced by a trustworthy third force with a service provider, which means a higher level of confidence should be assumed. Other techniques used ciphertext-policy ABE instead, where it is connected by the access policy with the ciphertext but not with the secret keys. Based on PRE and ABE, we will present a time-constrained access control mechanism. To update the time characteristics PRE can be used while to utilised to build time-based access control policies ABE is used. Even though these systems have led, but in the context of IoT, due to high computational costs of encryption and decryption they are not appropriate [1][2][4].

An Identity based proxy re-encryption scheme is appropriate for data sharing will be described. To the specific ciphertext the re-encryption keys are connected and the re encryption keys are also connected to user's identities. Hence now for each combination of data user and shared file a unique re-encryption key is generated by data owner. A near approach was offered, where this time a hierarchical PRE is employed instead of an identity-based PRE. When dealing with many and complicated data sets, these two techniques are inefficient. For data sharing, an identity-based broadcast encryption (IBBE) with PRE IBBE is also proposed where it is about broadcast encryption [1][3].

Their solution was a hybrid that allowed the two protocols to be converted without disclosing any critical information. We will also create an identity-based proxy RE mechanism for gaining access to records related to medical. The proposal was successful in providing bristly-grained access control.

If the re-encryption key from the data holder is obtained from proxy, either all or none of the ciphertexts are made available to the selected users and also can be encrypted again. On that basis, an IBEPRE scheme can be selected based on criteria. According to the concept, a portion of ciphertexts under one identity to ciphertext under another might get translated by proxy. Although, a set of users getting themselves granted decryption privileges was not possible. In addition to the foregoing, to control IOT issues PRE is being utilised [3].

To assure privacy and high private data management we can use block chain technologies well. There was no need for the third party because the blockchain was leveraged as an autonomous access control manager. The address that was kept by the blockchain was data address, a distribute hash table is the location where the data is stored. Hence the data has lowered.

Here is an example of a similar concept where inside the cloud we can see that the cryptosystem is uploaded and on the blockchain data access controls are being kept as transactions. Now simple auditing and tamperproof system is created by these two techniques, and access policies are created by these techniques because they leak because the blockchains employed are public which can result in that they are available and visible to everyone. In automobile

networks, and secure communication between vehicles abut data exchange we use a paradigm based on block chain. Although, there is the problem of high cost in construction, in resource constrained cars a blockchain is seen and also in peer-to-peer data exchange between cars or automobiles we do not see the blockchain function usage [5].

4. Proposed System

Caching is an ICN feature that enables material to be served from any intermediary device. One of the major prerequisites for a good ICN implementation is efficient caching [5]. For balanced content or data delivery in between devices on networks the caching techniques can be in use in this study. The selection of contents to be cached is defined by using Zipf's law [5].

The vigorous change in demand of items is taken into consideration while making caching selections. Every router monitors the cache state of its neighbours in order to balance the cached material throughout the network. To choose a router for caching contents, three criteria are considered: the proportional distance of the router from the client (pd), the router congestion (arc), and the cache status (cs). By using ndnSIM-2.0, the novel caching strategy is tested in a simulated environment. Three cutting-edge techniques are compared: Leave Copy Everywhere (LCE), a centrality measures-based algorithm (CMBA), and a probability-based caching (precache)[5].

The system presents a safe access control architecture to ensure confidentiality of data and fine-arranged access of data [5][4]. This also ensures that data owners can control their data totally. The system provides a good understanding about PRE scheme and also about the protocol which promises data confidentialities and privacy's implementation.

Here Edge devices perform as nodes that can be proxy and to optimise data delivery the cached data is re-encrypted which can result in making better use of network resources. There is greater computing capability in edge devices than IoT devices which results in enabling high performance networking. We offer our scheme's security analysis and test and evaluate its effectiveness with current schemes.

5. Advantages

1) MITM attacks which can be abbreviated as Man-in-the-Middle are not possible with the suggested solution. MITM attacks gain access to the certificate authority (CA) and supply fake public keys to the user.

2) When attackers infiltrate into system, their own copies of data will be injecting their own copies of the data into the system, which the suggested system detects and prevents.

3) The caching approach discussed in this work is divided into two stages. The first step identifies what material should be cached, and then in the second stage it chooses a suitable router where the content can be stored [5].

4) Here suggested method is the type of caching that is in-network in-network based on popularity. However, rather than random caching, this strategy focuses balanced content caching throughout the network[5].

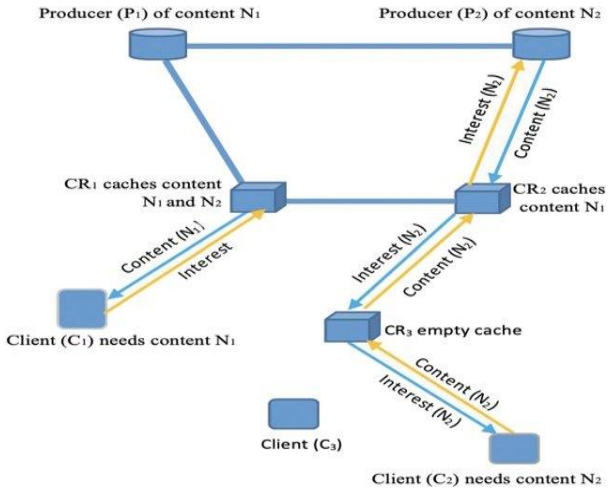

Figure 1. System process

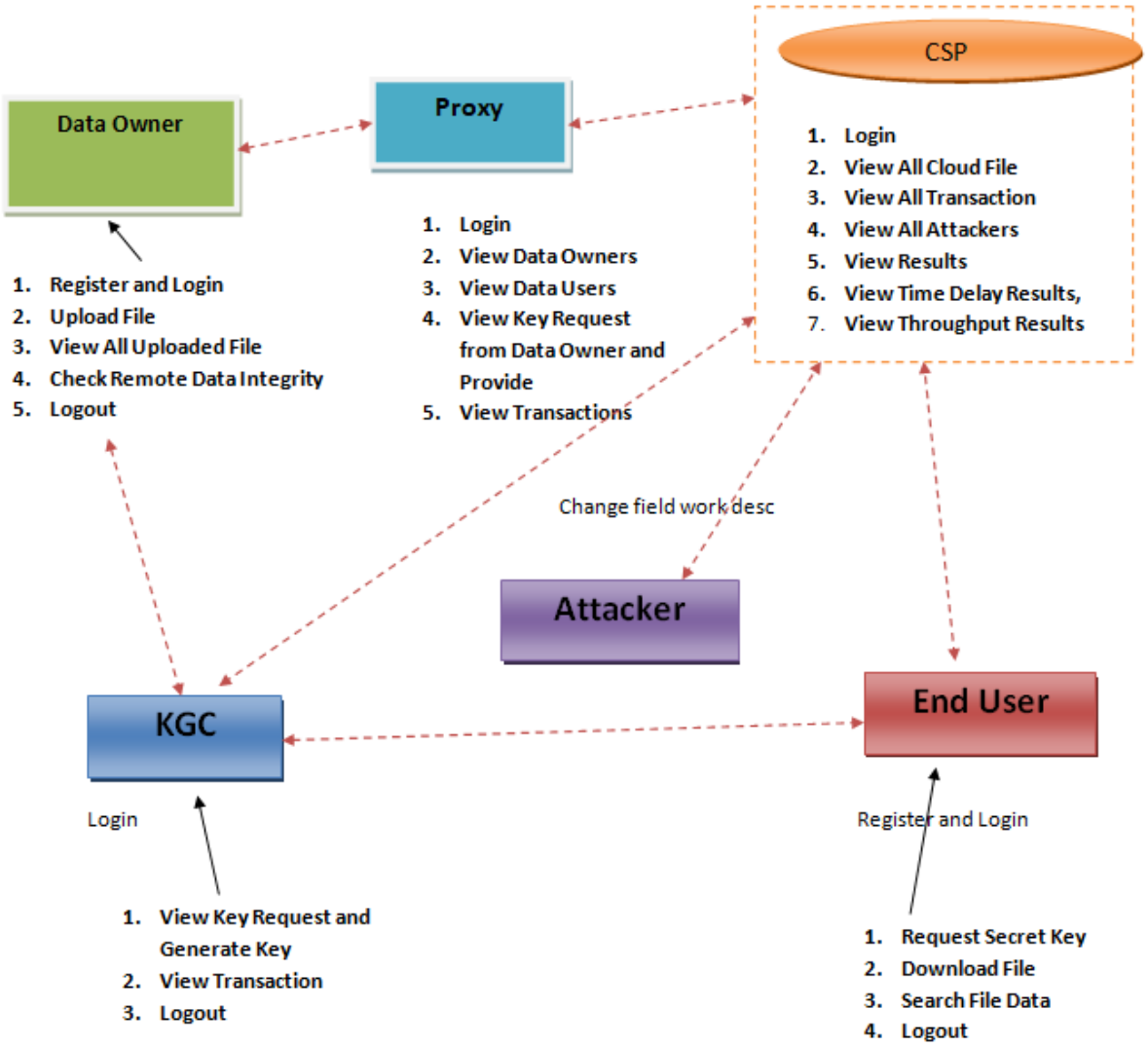

Figure 2. Flow model

6. Conclusion

Data sharing has emerged as one of the most notable uses of the Internet of Things. To make sure about data integrity, data confidentiality, and data privacy, in a cloud computing we can see that how a secure identity-based PRE mechanism which is works in data sharing can be shown. By using the IBPRE scheme the developers can allow the data owners to share their encrypted and secure data in the cloud and also, they can ably exchange it with authorised and accessed users, where the data is shared. For heavy calculations edge devices acts as the proxies because of the asset's limits. The method also combines ICN characteristics to efficiently transport cached material, hence enhancing service quality and making efficient use of network traffic [5].

Following that, we provide a system paradigm that is based on a blockchain where on an encrypted data a flexible authorisation is enabled. Fine-grained access control is established, and it can assist data owners in achieving acceptable privacy protection. The suggested model's study and results demonstrate how efficient our scheme is in comparison to existing systems. The introduction of ICN and its complete deployment appear to herald a paradigm change in Internet technology. In terms of network burden, data access would be lot cheaper, and distribution would be considerably quicker. Caching is the primary important procedure in igniting ICN's success. In this study effort, a caching strategy is developed with content popularity as the major foundation [5].

When storing material in the network, to prevent the caching of the same information in router, enormous caution is taken and it helps in equalizing data or information delivery across the network. The most important characteristics, such as the cache status and congestion of the present CR, as well as the condition of the content in the other adjacent router, are considered while selecting whether to store material. The first section of the study presents two algorithms for the proposed system. In nanism, the approach is simulated, and the results are compared to procache, cent Cache, and LCE. Observation demonstrates that the suggested protocol outperforms the other three techniques.

The incorporation of proportional distance, network congestion, and cache state during the content caching decision-making process is a strength of our method.

References

[1]. Saifullah khan, Akanksha Jadhav, Indrajeet Bharadwaj, Mayuk rooj, Sandeep Shira vale, "Block chain and Identity based encryption scheme for high data security", ICCMC, (2020).

[2]. Shangping wang, Ying long Zhang, Yaling Zhang," A blockchain based framework for data sharing with fine grained access control in decentralised storage systems", IEEE institute of electrical and electronics engineering (2018).

[3]. Kwame opuni, Qi Xia, Emmanuel Boateng, Christian cobblah, Hu Xia, Jianbin gao, "Proxy re-encryption approach to secure data sharing in the internet of things based on block chain", IEEE Creative commons attribution 4.0 international (2022).

[4]. Damiano Di Francesco, Paolo Mori, Laara Ricci," Blockchain based access control Used Access control-based schemes for data user", IEEE Creative commons attribution 4.0 international (2022).

[5] Andreana loanou, Stefen weber, "Towards on-path caching alternatives in Information-Centric Networks" 39th Annual IEEE Conference on Local Computer Networks (2014).

[6]. M. Prasad, "Promising Innovative Educational Applications Using Block Chain Technology & Issues", in BLAB – SAP 2019 held on 5-6 July,2019 at AKNU, Rajamahendravaram.

[7]. M. Prasad, Mallikarjuna Reddy A, Srinivas Reddy K, "Internet of Things (IoT) Security Threats and its Countermeasures", International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 8, Aug 20, ISSN NO: 0976-6499.

