Chapter 11
Efficient Data Verification Systems for Privacy Networks

Vinoth kumar V.
Jain University, India

Muthukumaran V.
https://orcid.org/0000-0002-3393-5596
REVA University, India

Rajalakshmi V.
REVA University, India

Ajanthaa Lakkshmanan
Annamalai University, India

Venkatasubramanian S.
Saranathan college of Engineering, India

Mohan E.
Lord Venkateswara Engineering College, India

ABSTRACT

To overcome the problem with aggregated raw data, privacy preservation is the best answer. For privacy measures and other concerns, it delivers full throttle security for data. The essential reason for data security is that single transactions will not be permitted and recently utilised customers to communicate information securely. This study presents and compares various verification strategies based on the crypt arithmetic methodology for various set-valued data. It primarily checks for privacy risks in the sharing of details and information between the publisher, admin, and customers. There are various ways of preventing privacy violations, including the PPCDP technique for strong data that is non-trivial to implement. The authors used the Java Tomcat server, HTML, and JavaScript to develop a web application. We can automatically stop the person who is attempting to inject the vulnerability code using the technique, and all of this information is kept in the database.

DOI: 10.4018/978-1-7998-9640-1.ch011

INTRODUCTION

The method of privacy preserving public key encryption standard uses cryptographic method to provide security for multiple users .For example Facebook is the biggest trusted web application in which it incubates billions of users send it doesn't provide security to all users .In spite of that we have created a small web application that will provide a full security for the customers in additional to encryption standard .It include all concepts of providing security like storing the data in cloud exchanging the bank details using random key generation for single user etc. Security ensuring utility check framework reliant on cryptographic methodology for differentially private arrangement planned for set the data. It measures on the encoded rough publishers which ensure break is engaged to covertly check the rightness of the mixed frequencies gave by the distributer, which perceives users. It provides the strengthened framework to another differentially private conveying plan proposed for data security (Muthukumaran V et al., 2018). Our speculative and preliminary evaluations display the security and capability of the proposed framework.

We propose the triple DES and RSA security algorithms to provide security based on the users request. In which user can buy the products or books securely based upon the user request to complete the transaction and payment gateway to send the book with key to view completely to the user (Muthukumaran V et al., 2021). We have created a java-based web application using tomcat SQL server, JavaScript html and CSS, where the user can be able to search for the websites, admin can be able to block the particular website and the owner can be able to host the website and all the details were stored in the database (Kumar, V et al., 2021; Nagarajan, S. M et al., 2022). As distributed computing becomes more widespread, more sensitive data is being gathered and shared in the cloud, posing new challenges for re-appropriated information security and protection. Property-based encryption (ABE) is a promising cryptographic approach that has recently been widely used to implement a fine-grained access control system. In any case, ABE is being chastised for its high plan overhead as the computing cost grows as the entrance equation becomes more complex. Since cell phones have compelled figuring assets, this disadvantage is becoming increasingly apparent.

With the increasing development of large-scale websites like DeForge's, java tpnint, beginners book etc., millions of people can share any kind of knowledge each other. People can share new ideas, innovations and hot topics. However, spreading information cause serious issue in society. So, it is important to identifying this kind of malicious users. Once the user detected it should be stopped as soon as possible and the negative influence to be reduced. Blocking certain subset of nodes will helps to reduce malicious user propagation. Most of the work concentrated on maximizing the influence of positive information through social websites based on lC model. On the other side, the negative influence minimization problem has less attention. So, it needs consistent efforts on strategies for blocking malicious users and minimizing the influence of those users.

We present limit DSS (Digital Signature Standard) marks where players share the ability to sign with the goal of fundamentally improving for a given parameter t over an ongoing result by Langford from CRYPTO'95 that presents limit DSS marks that can stand a lot smaller subsets of debased players, specifically tpn, and despise the power property. Because of Langford's outcome, our strategies do not necessitate a trusted third party. Our solutions are also applicable to additional ElGamal-like edge marks. We show that the security of our plans is solely determined by the difficulty of generating a standard DSS signature.