TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS

[1] Prof Ch.G.V.N Prasad,[2] G. Sri Harsha,[3] G. Yugendar Reddy,[4] G. Sai Ram,[5] G. Devendar Yadav
[1] Assistant Professor,[2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

Transactions form the core of economic activities, representing the intricate interplay between buyers and sellers. The concept of Exchange Liability comes into focus as these transactions unfold within the context of Deceitful Big Data, where manipulation and misinformation threaten the trust upon which commerce relies. The ramifications of misrepresentation or falsification of information lead to Adverse effects, impacting both parties involved and potentially causing larger disruptions across the market ecosystem. The proliferation of Big Data has transformed consumer-retailer relationships, enabling personalized experiences and informed decisions. However, the interplay between Deceitful actors within this data-driven landscape necessitates a comprehensive exploration of liability. This study navigates the nuances of liability in transactions involving Big Data Consumers and retailers, taking into account the challenges posed by data authenticity, transparency, and trustworthiness. Through a synthesis of legal considerations, ethical perspectives, and technological implications, this research delves into the multifaceted nature of liability in Transaction Exchange within the realm of Deceitful Big Data. By elucidating the responsibilities and potential consequences, the study aims to shed light on strategies that can be adopted to mitigate risks, foster transparency, and promote fair interactions between consumers and retailers.

Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges. Some existing remote integrity checking methods can only serve for static archive data and thus cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper, we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

I. INTRODUCTION

In an era defined by rapid technological advancements and interconnectedness, the dynamics of commerce and data exchange have undergone significant transformations. The intricacies of modern transactions extend beyond the traditional exchange of goods and services, encompassing the digital realm where vast amounts of data are shared, analyzed, and acted upon. This evolution brings with it a multitude of challenges and opportunities, particularly in the realm of liability within the context of Transaction Exchange involving Deceitful Big Data Consumers and retailers.

The process of Transaction Exchange lies at the heart of economic activities, shaping the interactions between consumers and retailers in a global marketplace. With the advent of Big Data, this exchange has taken on new dimensions, enabling personalized recommendations, tailored experiences, and data-driven decision-making. However, the pervasive nature of Deceitful practices within this landscape poses intricate questions about accountability and liability. Liability, as a concept, embodies the responsibilities and consequences that arise from actions taken within transactions. In the context of Deceitful Big Data Consumers and retailers, the challenge lies in navigating the intricate terrain where information can be manipulated, obscured, or exploited for personal gain. The implications of misrepresentation or dishonesty ripple through the ecosystem, impacting the trust and integrity upon which commerce thrives. This study aims to unravel the layers of liability within the landscape of Transaction Exchange involving Deceitful Big Data Consumers and retailers. By delving into the intricacies of this topic, we seek to address fundamental questions about ethical standards, legal considerations, and technological safeguards that underpin the interactions between parties. Through a multidisciplinary exploration, we aim to shed light on the responsibilities that accompany the exchange of data-driven insights and to propose strategies that foster transparency, fairness, and accountability. Each transaction becomes a data point, contributing to the creation of comprehensive consumer profiles. Retailers, armed with sophisticated analytics, utilize this information to personalize experiences, optimize marketing strategies, and enhance overall operational efficiency. Despite the promising aspects of this synergy, the underbelly of big data reveals a darker side. Deceitful practices, ranging from unauthorized data collection to intentional misinformation, have become prevalent. Consumers, often unknowingly, find themselves at the mercy of entities that exploit their personal information for profit. Retailers, too, may fall victim to deceptive practices within their supply chains or among third-party data processors.

The concept of transaction exchange liability encompasses the responsibility borne by both consumers and retailers in the event of deceitful big data practices. Consumers face the risk of financial loss, identity theft, and compromised privacy, while retailers grapple with reputational damage, legal repercussions, and potential financial liabilities. The evolving nature of these threats necessitates a comprehensive understanding of the intricate legal and ethical dimensions surrounding transactional data exchange.

As the symbiotic relationship between transactions and big data continues to shape the future of commerce, the potential for deceitful practices casts a looming shadow. Understanding and mitigating transaction exchange liability is a shared responsibility that requires collaboration between consumers, retailers, and regulatory bodies. In the pages that follow, we will delve deeper into the intricacies of this multifaceted issue, exploring its implications, legal frameworks, and potential solutions in the quest for a more secure and ethical transactional landscape.

Consumers, on the other hand, face the challenge of trusting retailers with their data. The risk of their information being used deceptively or without consent raises concerns about privacy, security, and the potential consequences of such misuse. Adverse outcomes in transaction exchanges can include financial losses, compromised personal information, erosion of trust between consumers and retailers, and reputational damage. When deceitful practices or breaches occur, the liability for such actions becomes a critical point of discussion, determining who holds responsibility and accountability for the consequences.

To address these challenges, regulators, policymakers, and industry stakeholders are working on establishing frameworks, standards, and regulations to govern the ethical use of big data in transactions. Companies are also implementing measures such as transparent data policies, robust security protocols, and ethical guidelines to protect consumer interests and ensure fair, secure, and responsible exchanges.

II. LITERATURE SURVEY

TITLE: Data markets compared.

AUTHOR: A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash,

ABSTRACT: The sale of data is a venerable business, and has existed since the middle of the 19th century, when Paul Reuter began providing telegraphed stock exchange prices between Paris and London, and New York newspapers founded the Associated Press. The web has facilitated a blossoming of information providers. As the ability to discover and exchange data improves, the need to rely on aggregators such as Bloomberg or Thomson Reuters is declining. This is a good thing: the business models of large aggregators do not readily scale to web startups, or casual use of data in analytics.

TITLE: Ftc charges data broker with facilitating the theft of millions of dollars from consumers' accounts.

AUTHOR: M. Blaze, G. Bleumer, and M. Strauss,

ABSTRACT: A data broker operation sold the sensitive personal information of hundreds of thousands of consumers – including Social Security and bank account numbers – to scammers who allegedly debited millions from their accounts, the Federal Trade Commission charged in a complaint filed today. According to the FTC's complaint, data broker LeapLab bought payday loan applications of financially strapped consumers, and then sold that information to marketers whom it knew had no legitimate need for it. At least one of those marketers, Ideal Financial Solutions – a defendant in another

FTC case – allegedly used the information to withdraw millions of dollars from consumers' accounts without their authorization. "This case shows that the illegitimate use of sensitive financial information causes real harm to consumers," said Jessica Rich, Director of the Federal Trade Commission's Bureau of Consumer Protection. "Defendants like those in this case harm consumers twice: first by facilitating the theft of their money and second by undermining consumers' confidence about providing their personal information to legitimate lenders."

The defendants collected hundreds of thousands of payday loan applications from payday loan websites known as publishers. Publishers typically offer to help consumers obtain payday loans. To do so, they ask for consumers' sensitive financial information to evaluate their loan applications and transfer funds to their bank accounts if the loan is approved. These applications, including those bought and sold by LeapLab, contained the consumer's name, address, phone number, employer, Social Security number, and bank account number, including the bank routing number.

TITLE: Ftc complaint offers lessons for data broker industry

AUTHOR: A. Shamir,

ABSTRACT: Two weeks ago, the FTC filed a district court complaint in Arizona against an operation that included three corporations and one individual. While touted as a case against data brokers ("FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts"), the single count unfair trade practices action really involves fraudulent and egregious conduct that took advantage of a particularly vulnerable population, but it nevertheless provides a few lessons for the data broker industry generally. Financially strapped individuals visited payday loan websites that promised to help them obtain payday loans if they filled out online applications and provided information such as name, address, phone number, employer, SSN, and bank account numbers that often included a bank routing number. These websites sold the pay day loan applications to data brokers. The defendants in this case purchased the application information from other data brokers, not the payday loan websites.

The defendants then sold the applications to both lenders, often for as much as $10 to $150 per lead, and non-lenders. The focus of the FTC's complaint is the application information that was sold to non-lenders. According to the complaint, from 2006 to 2013 the defendants sold 95% of the applications for about 50 cents each, sometimes multiple times, to non- lender third parties some of whom the defendants knew were engaged in fraud. Specifically, the complaint alleges that the individual who controlled the corporations was aware that one of the entities that purchased the application information, Ideal Financial and its web of corporations and individuals, was engaged in a fraudulent billing and debiting scheme.

TITLE: Multimedia computing and computer vision lab

AUTHOR: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano,

ABSTRACT: The Multimedia Processing and Computer Vision laboratory is widely known as one of the best of its kind in the UK and has also earned international recognition. Its work has involved collaboration with industrial partners and academics from UK and abroad. Its ongoing research covers a broad spectrum of computational techniques associated with visual and audio media, from video compression to medical image processing.

A particular feature of our work over in past 20 years has been the use of multiresolution signal representations. These include wavelets and related transforms for compression and segmentation and 'coarse-fine' methods for estimation of disparity fields in such areas as stereopsis and visual motion.

We have collaborated with many other research groups within the University of Warwick, including the Mathematics Institute and the Departments of Statistics and Psychology, University Hospitals of Coventry and Warwick and at other Institutions, including Yale, Harvard, Zurich and Bristol Universities, the Institute of Psychiatry and organisations such as Oxford GlycoSciences Ltd, Sony Broadcast and Professional (Europe), DERA Malvern (now QinetiQ) and the Forensic Science Service. Recently we have been involved in several projects with Warwick Medical School, Pattern Analytics Ltd, and Jaguar Land Rover research.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

One of the major concerns is that we do not have accountability in the digital data trading. The concerns are particularly huge due to the non-physical nature of the digital dataset – replication and delivery are almost costless when compared to physical commodities. Concerns arise at the broker side: data owners worry that brokers may illegally disclose or resell the datasets they outsourced to the brokers. On the other hand, concerns arise at the consumer side as well: dishonest consumers may illegally resell the purchased datasets.

Deceitful big data consumers could exploit vulnerabilities in the existing system. They might engage in fraudulent transactions, manipulate data, or exploit loopholes in the exchange process. Determining liability in the face of deceitful practices becomes challenging. Retailers may find it difficult to identify and hold deceitful consumers accountable for their actions, leading to financial losses and reputational damage. Deceitful big data consumers might compromise the security of sensitive information, posing risks to both retailers and other consumers. This could lead to identity theft, financial fraud, or other malicious activities. The existing system must comply with relevant regulations regarding data protection, consumer rights, and business practices. Non-compliance could result in legal consequences for both retailers and deceitful big data consumers. Retailers may need to implement robust security measures, fraud detection systems, and ethical data usage policies. Regular audits and monitoring can help identify and address deceitful practices. Advanced technologies, such as blockchain for secure transactions or artificial intelligence for fraud detection, can enhance the resilience of the existing system against deceitful behavior. The existing system refers to the infrastructure, processes, and technologies currently in place for conducting transactions, managing data, and ensuring the smooth operation of business activities.

DISADVANTAGES OF EXISTING SYSTEM:

- Data owners worry that brokers may illegally disclose or resell the datasets they outsourced to the Brokers
- Concerns arise at the consumer side as well: dishonest consumers may illegally resell the purchased datasets.
- Incidents involving deceitful practices, especially if they become public, can severely damage a retailer's reputation. Consumers may lose trust, affecting customer loyalty and the overall brand image.
- Deceitful practices may involve the misuse of consumer data. This can result in data breaches, identity theft, and privacy violations, causing harm to individuals whose information is compromised.
- Despite the implementation of liability measures, deceitful practices can still occur. Some measures might create a false sense of security for consumers, leading them to believe their data is completely safe, while in reality, breaches and deceitful practices could still happen.

PROPOSED SYSTEM

- Propose a suite of accountable protocols, denoted as Account Trade, for big data trading hosted by data brokers. Account Trade enables brokers to attain accountability against dishonest consumers throughout the trading by detecting their misbehavior.
- The trading-related misbehavior defined in this paper includes tax evasion, denial of purchase, and resale of others' datasets.
- Note that we do not try to detect idea-wise plagiarism (e.g., novels with similar plots, images taken at the same scenery spot, videos taken with similar angles) because originality is a subjective factor that is hardly decidable even by human.
- Instead, we propose to detect the blatant copy (not an exact copy) in the datasets uploaded by owners, by detecting whether the given datasets are derived from others that have been uploaded before.
- Notably, the fuzzy copy-detection in table-type datasets or JSON-like datasets has not been studied yet to the best of our knowledge, and Account Trade is the first to propose a feasible mechanism.
- Retailers should establish and communicate clear, concise, and easily accessible data policies. These should inform consumers about the type of data collected, how it's used, and with whom it's shared.
- Establish guidelines for the ethical use of big data, ensuring that the data collected is used responsibly and for legitimate purposes. This includes prohibiting the manipulation or exploitation of consumer data for misleading or deceitful practices.
- Empower consumers through education. Retailers should provide resources that help consumers understand their rights, how their data is used, and how to protect themselves from deceitful practices.
- Engage independent third-party auditors to oversee and verify that retailers adhere to ethical data practices. This helps in maintaining accountability and trust in the system.

- Combining these measures can contribute to a more ethical and secure environment for transaction exchanges involving big data. Collaboration between retailers, consumers, regulators, and technology experts is key to ensuring the success of such a system and fostering trust in the marketplace.

ADVANTAGES OF PROPOSED SYSTEM:

- AccountTrade which guarantees correct book-keeping and achieves accountability in the big data trading among dishonest consumers
- AccountTrade blames dis-honest consumers if they deviate from their responsibilities in data transactions
- Consumers are safe from fraud activities or misuse of their data, ensuring their rights and privacy are upheld during transactions.
- Big data allows retailers to implement personalized security measures based on individual consumer behavior. This includes adaptive authentication methods, reducing the likelihood of unauthorized access.
- The use of big data enables real-time monitoring of transactions. Suspicious activities can be identified and addressed promptly, preventing further damage and losses.

Big data facilitates continuous improvement in fraud prevention strategies. Analyzing historical data and adapting to emerging patterns allows retailers to stay ahead of evolving deceitful practices.

SYSTEM ARCHITECTURE

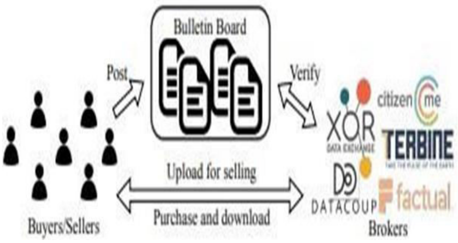


Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- Buyer
- Seller
- Admin
- Broker
- Accountability

MODULE DESCRIPTION

Buyer

The buyers should register with the application and the buyer should authorize by the admin then only the buyers can login into his home page. Here the buyers can update his details to purchase the shares based on his capacity.

Seller

In this application the seller should register with the application and the seller should authorize by the admin then only the seller can able to login into the application. And the seller can post the shares and the share value to the admin. And also check the share-holder of his company.

Admin

In this application the admin can directly login into the application and authorize the sellers and buyers and the admin can share all the company shares to the broker. And the admin can also check the dishonest users.

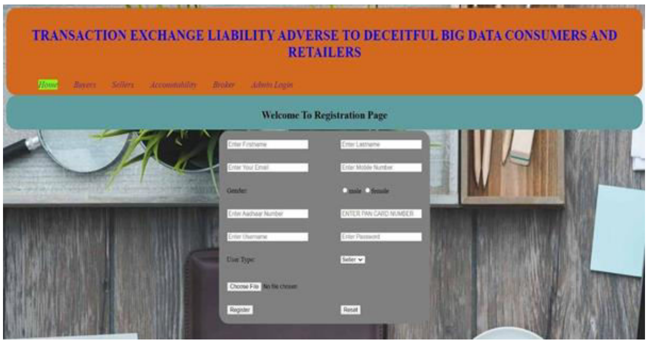
Broker

Here the broker is also one of the modules and the broker can share all the company shares to the buyers based on the buyers capacity and also share all the shares to the buyer.

Accountability

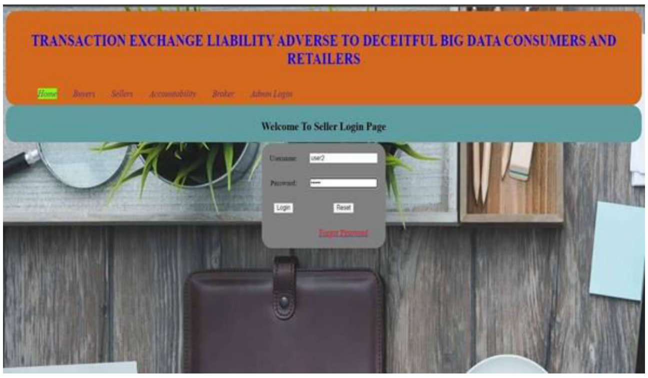
Here the accountability module can check the dis-honest persons.

V. SCREENSHOTS:


TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS
Home
Buyers
Sellers
Accountability
Broker
Admin Login
Register
Reset
Choose File

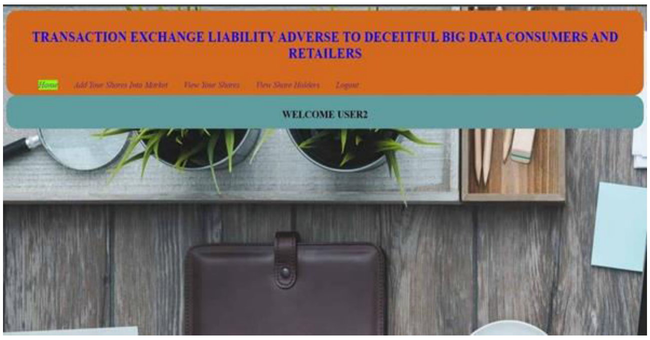
Welcome To Registration Page

Enter Firstname | Enter Lastname
Enter Your Email | Enter Mobile Number
Gender: ○ male ○ female
Enter Aadhaar Number | ENTER PAN CARD NUMBER
Enter Username | Enter Password
User Type: Seller
No file chosen

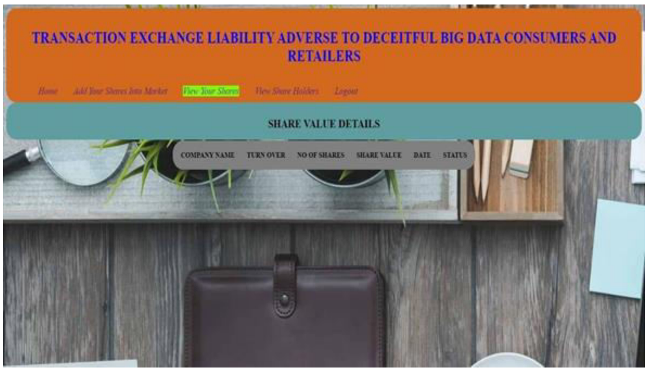

TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS
Home
Buyers
Sellers
Accountability
Broker
Admin Login
Login
Reset
Forgot Password

Welcome To Seller Login Page

Username: user2
Password: ••••

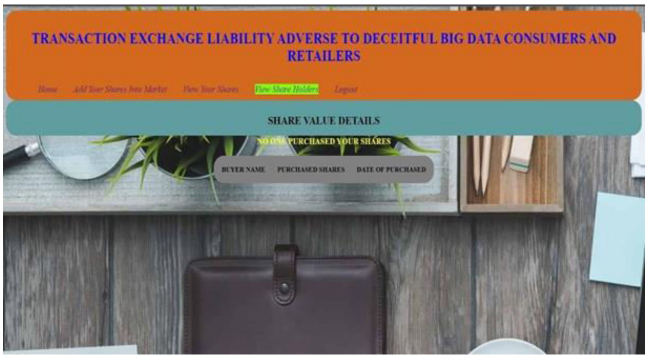

TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS

WELCOME USER2


TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS

SHARE VALUE DETAILS

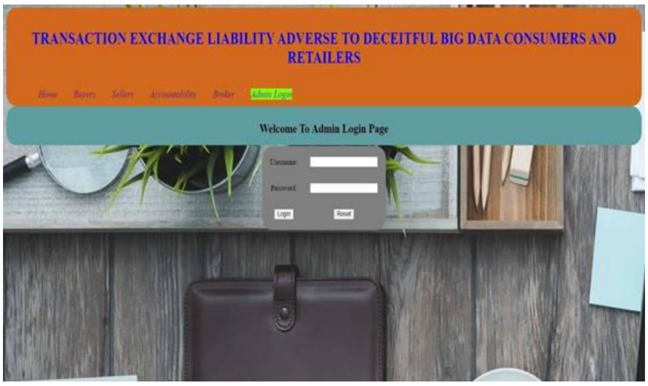
COMPANY NAME	TURN OVER	NO OF SHARES	SHARE VALUE	DATE	STATUS


TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS

SHARE VALUE DETAILS

NO ONE PURCHASED YOUR SHARES

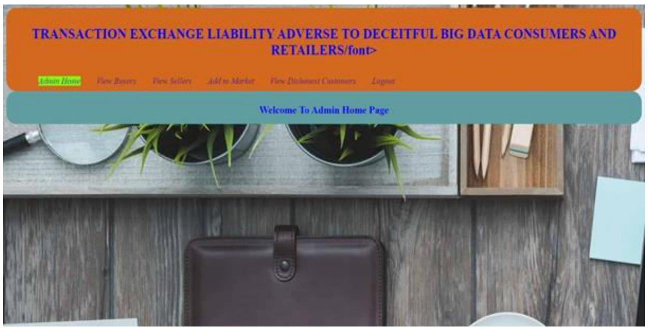
BUYER NAME	PURCHASED SHARES	DATE OF PURCHASED


TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS

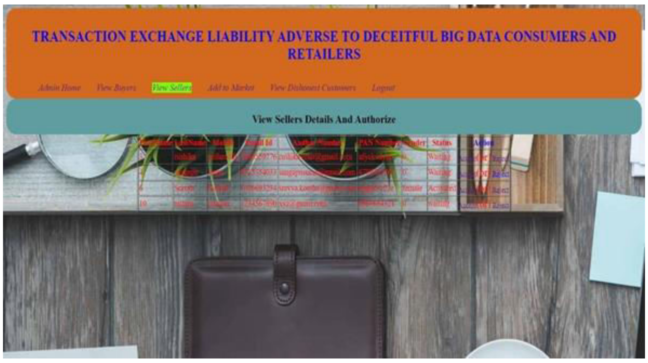
Welcome To Admin Login Page

Username:

Password:


TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS/font>

Welcome To Admin Home Page


TRANSACTION EXCHANGE LIABILITY ADVERSE TO DECEITFUL BIG DATA CONSUMERS AND RETAILERS

View Sellers Details And Authorize

VI. CONCLUSION

CONCLUSION

This paper presents AccountTrade which guarantees correct book-keeping and achieves accountability in the big data trading among dishonest consumers. AccountTrade blames dishonest consumers if they deviate from their responsibilities in data transactions. To achieve accountability against dishonest sellers who may resell others' datasets, we presented a novel rigorous quantification of the dataset uniqueness – uniqueness index – which is efficiently computable. We formally defined two accountability models and proved them with ProVerif and theoretic analysis, and we also evaluated the performance and QoS using real- world datasets in our implemented testbed.

FUTURE SCOPE

The future scope for a transaction exchange system designed to mitigate liability risks associated with deceitful big data consumers and retailers lies in the continual advancement of artificial intelligence (AI) and machine learning (ML) technologies. Implementing more sophisticated algorithms for fraud detection and prevention, leveraging predictive analytics to identify evolving patterns of deceit, and enhancing anomaly detection capabilities will be pivotal. Additionally, exploring blockchain technology for secure and transparent transaction records can provide an immutable ledger, further bolstering trust. Collaboration with regulatory bodies to ensure compliance with emerging data protection and privacy laws will be essential. Furthermore, integrating advanced biometric and behavioral analytics for user authentication and continuous monitoring can enhance the security posture of the system. As the digital landscape evolves, incorporating these cutting-edge technologies and staying abreast of emerging threats will be key to maintaining the resilience and effectiveness of the transaction exchange platform in safeguarding against deceitful practices in the realm of big data transactions for both consumers and retailers.

REFERENCES

1. Data markets compared – a look at data market offerings from four providers. goo.gl/k3qZsj.
2. Ftc charges data broker with facilitating the theft of millions of dollars from consumers' accounts. goo.gl/7ygm7Q.
3. Ftc charges data brokers with helping scammer take more than $7 million from consumers' accounts. goo.gl/kZMmXn.
4. Ftc complaint offers lessons for data broker industry. goo.gl/csBYA3.
5. Multimedia computing and computer vision lab. goo.gl/pbKeCj.
6. R. Araujo, S. Foulle, and J. Traor ´ e. A practical and secure coercion- ´ resistant scheme for remote elections. In Dagstuhl Seminar Proceedings. Schloss Dagstuhl-Leibniz-Zentrum fur Informatik, 2008. ¨
7. D. Baltieri, R. Vezzani, and R. Cucchiara. Sarc3d: a new 3d body model for people tracking and re-identification. In ICIAP, pages 197– 206. Springer, 2011.
8. B. Blanchet. Automatic verification of security protocols in the symbolic model: The verifier proverif. In FOSAD, pages 54–87. Springer, 2014.
9. B. H. Bloom. Space/time trade-offs in hash coding with allowable errors. Communications of the ACM, 13(7):422–426, 1970.
10. S. Brin, J. Davis, and H. Garcia-Molina. Copy detection mechanisms for digital documents. In SIGMOD, volume 24, pages 398–409. ACM, 1995.