M. Mohanedova *et al*, International Journal of Advances in Agricultural Science & Technology,
Vol.11 Issue.4, April 2024, pg. 65-70

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

A novel application for analysing customer revies using Blockchain

Mr.A.Avinash [1] , Sigala Sri Chaitanya Kumar [2], Kaki Lalitha Sri Sai Manasa [3], Kondayyapalepu Ambica [4], Badala Dintu Deekshith [5], Kotipalli Ananta Sai Lakshmi Durga [6] , [1]Assistant Professor , [2, 3, 4, 5, 6]B.tech Students
Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India Email: avinash.a@pragati.ac.in

Abstract:

Consumers can make informed purchase decisions and learn more about things by sharing their experiences with others through user reviews. To enhance their business, internet retailers and service providers may modify customer evaluations by adding false positive remarks and removing negative ones. Customer reviews that have been edited may mislead customers and alter the original content of the reviews. Modern systems lack a safe, effective, and user-friendly consumer review system. In this work, we provide RevBloc, a highly efficient, secure, and easy-to-use customer review system. Because RevBloc is built on blockchain technology, user evaluations can be maintained in a distributed ledger, preventing a single or small number of unfriendly parties from influencing the reviews. We implement a RevBloc proof-of-concept prototype and describe its performance to illustrate the strategy's practicality.

Keywords: RevBloc**,** blockchain technology, proof-of-concept

I. Introduction

Clients find it easier to use online services; but, because they cannot check the quality of a product or service, they may wind up purchasing something that does not fit the description. To alleviate this concern, online shops and service providers allow customers to share both positive and negative experiences with new customers. According to Gartner [1], reputable customer reviews have the potential to increase an online product seller's customer base and attract new ones. Customers can learn more about products and services by reading user reviews. As a result, clients may feel more empowered to make wise and confident purchasing decisions and use services. Positive customer reviews have the ability to greatly increase online product consumption while also establishing a positive reputation for the sellers. Unfavourable client feedback, on the other side, may help them identify which services need to be improved. To put it another way, client reviews can be used to solicit feedback as well as to demonstrate their social standing. Unfortunately, malicious actors can add, alter, remove, and conceal consumer reviews in order to manipulate them. For example, even if a seller's items are of great quality, potential customers may see poor reviews and be swayed to make a purchase if a malicious party, such as a competitor, posts negative information about them. A fake evaluation would hurt the seller's interests. In contrast, businesses trying to make a profit may spend money on false testimonials for their products. As a result, these positive reviews may inadvertently inspire more individuals to buy the goods immediately, perhaps increasing sales. Even worse, shops may be able to erase adverse assessments by paying someone to do so. Thus, modified customer reviews may mislead purchasers and alter the actual content of the reviews. Customer review integrity protection is in high demand. Data integrity has been the subject of various papers [2-9]. Numerous scholars have investigated secure logging as a popular data protection area [10]–[18]. However, these studies are not intended for customer review systems; rather, they focus exclusively on data integrity. More specifically, these studies do not explain how to maintain a system that is usable, efficient, and secure; how to ensure the authenticity of consumer feedback; how to decrease the danger of sensitive information leaking in transit; or how to accommodate multiple users. Although well-known worldwide online shops such as Amazon and eBay provide consumer review systems, the fact that these systems are self-managed allows for review manipulation. We recommend RevBloc as a solution for the problem of manipulated customer reviews since it provides a highly secure, effective, and user-friendly customer

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

review platform. We use blockchain technology to ensure the availability and preservation of customer review data in a decentralized storage system, preventing a single party from controlling the reviews. We use an Identity Provider (IdP) to allow users to manage only one password, which relieves the strain of having to establish and remember multiple passwords for different online services. Our technique is based on a compact password-authenticated key exchange protocol (CompactPAKE) [19].

II. LITERATURE SURVEY

Covert Key Administration. To achieve forward security, Schneier and Kelsey [2] propose a hash chain approach based on Message Authentication Codes. This means that each subsequent data entry is connected with a hash key based on the previous entry. Bellare and Yee [3] offer a MAC-based forwarding security mechanism that ensures session keys stay secure even if the previous key is compromised. A number of secret sharing techniques, such as the one described in Shamir [4], have been devised to ensure that every user in the cloud environment has access to the secret. Secret sharing schemes do not protect data, however, because the secret can be reorganized if one of the servers hosting the secret sharing systems is compromised [5]. Gentry and Ramzan [8] propose an identity-based aggregate signature scheme that use two constant-length 'tags' rather than different signer public keys for data verification. As a result, collecting and maintaining the public keys is not required to ensure the accuracy of the data. Safe record-keeping. To ensure the log record's integrity, BBox [10] relies on the hash function and the Device Authorization and Key Lookup (DAKL) table, both of which are based on Schneier and Kelsey's research [2]. Stathopoulos et al. [20] use digital signatures in a unique approach to protect data integrity; that is, signatures can replace MACs in data verification. This approach uses a TTP to store integrity proofs and verify data integrity. To ensure the integrity of log data, Holt [11] proposes Logcrypt, a solution that builds on the concepts given in [22] and [2] by replacing MACs with digital signatures and ID-based encryption. However, because integrity protection in these solutions is based on a trusted environment, if the trusted components are compromised, attackers may be able to utilize them to modify data. Secure Logging-as-a-Service (SecLaas) [12] safeguards log integrity against dishonest investigators or cloud service providers (CSPs) by using Proofs of Past Log (PPL). After publishing the PPL, the PPL can ensure that CSPs cannot change the log records during the storage phase. Investigators can access the logs during the retrieval process by using the log API. Then, to ensure that the data logs are full, they evaluate the accuracy of the evidence as well as each individual log entry and record order. The Cloud Log Assuring Soundness and Secrecy (CLASS) method [13] takes an alternative technique that solves the flaws of the previous study SecLaas by generating PPL with the log chain to maintain the integrity of the log records. In terms of log processing, verification, and accumulator performance, CLASS surpasses SecLaas. The fact that all of the data can be maintained by a single business, allowing CSP some data control, is a key disadvantage of this strategy. A TTP module, such as a hardware or virtual module [23], can be used to provide secure log encryption capabilities in order to prevent log manipulation by companies. In an untrustworthy CSP context, Kunz et al. [14] offer a trustworthy logging mechanism based on the Schneier and Kelsey technique [7] to assure log entries' authenticity, forward integrity, and secrecy. CSPs simply ensure that all log entries are recorded in the log files. A TTP that is separate from the cloud party provides an important storage service. Similarly, the difficult issue of certificate management in traditional cloud data integrity testing protocols has been solved with the development of an identity-based cloud data integrity checking protocol (ID-CDIC) [15]. Furthermore, our research assumed that other platform players cannot be fully trusted and that the entity generating the private keys is a TTP. As a result, ID-CDIC used identity-based RSA signatures to verify the integrity of the outsourced data and the outsourced file tag to enforce authentication between parties. For distributed systems, the Blind-Aggregate-Forward (BAF) [16] audit logging mechanism is useful. An online TTP is not required for BAF to provide public verification. An offline TTP is also used to produce the private and public keys that signers and verifiers require.

III. SYSTEM ANALYSIS

A. EXISTING SYSTEM

The overarching subject matter of various works is data integrity. Numerous researchers have investigated secure logging as a key data protection domain. However, these studies are not intended for customer review systems; rather, they focus exclusively on data integrity. More specifically, these studies do not explain how to maintain a

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

system that is usable, efficient, and secure; how to ensure the authenticity of consumer feedback; how to decrease the danger of sensitive information leaking in transit; or how to accommodate multiple users. Although well-known worldwide online shops such as Amazon and eBay provide consumer review systems, the fact that these systems are self-managed allows for review manipulation. A comparative assessment of current approaches. We evaluated current choices in light of the specifications provided in Section II-B. Table I offers a comparison of the solutions. All of the system requirements listed in Section II-B are not supported by any of the solutions tested. All of these requirements are met by our solution.

DISADVANTAGES OF THE EXISTING SYSTEM

Limited Attention to Customer Review Systems: Previous research on data integrity and secure logging has focused on generic data protection rather than the specific demands of customer review systems. This restricted focus may lead key details specific to processing user-generated content and comments to be overlooked.

Insufficient Support for a Large Number of Users: Many current solutions fall short of meeting the scalability and multi-user help requirements for customer review systems running on large platforms. Scalability issues may arise when dealing with significant amounts of user-generated content and interactions.

Inadequate Authentication Mechanisms: Ensuring the legitimacy of consumer reviews is critical to maintaining review system credibility. However, current solutions may not have robust authentication methods in place to validate the integrity of people posting assessments, leaving the system vulnerable to fake and manipulative reviews.

Risk of Sensitive Information Leakage: While data integrity controls can prevent unauthorized users from making changes to data reviews, sensitive information may leak during data transmission. Existing solutions may fail to detect this risk. User data may be intercepted or accessed by unauthorized parties owing to insufficient encryption or security measures.

Usability and Efficiency Challenges: Certain solutions that are currently in use prioritize security over efficiency and usability. Robust authentication methods or complex security measures may deter user involvement and limit the review system's efficacy. Maintaining a balance between security and usability is critical for ensuring widespread acceptance and efficient operation.

B. PROPOSED SYSTEM

Covert Key Administration. To achieve forward security, Schneier and Kelsey propose a hash chain mechanism based on Message Authentication Codes (MAC). This technique requires that each subsequent data entry have an associated hash key that is dependent on the previous item. To ensure that session keys stay secure even if the previous key is compromised, Bellare and Yee offer a MAC-based forwarding security mechanism.

Covert Key Administration. To achieve forward security, Schneier and Kelsey propose a hash chain mechanism based on Message Authentication Codes (MAC). This technique requires that each subsequent data entry have an associated hash key that is dependent on the previous item. To ensure that session keys stay secure even if the previous key is compromised, Bellare and Yee offer a MAC-based forwarding security mechanism.

IV.SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

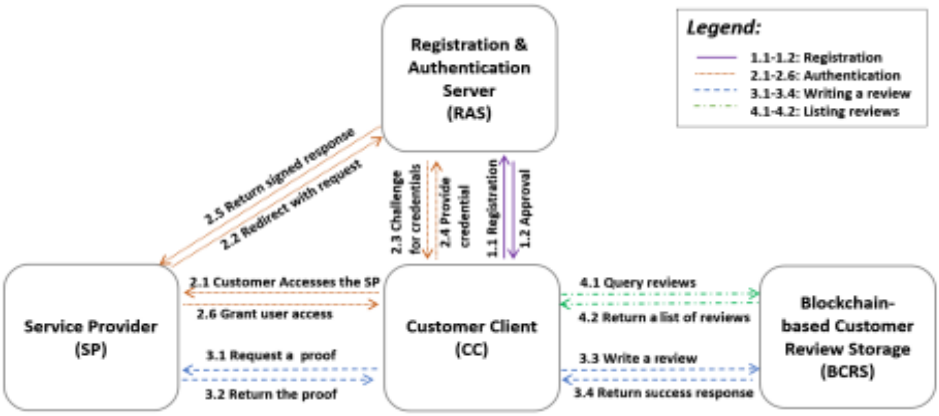


Fig 1. Methodology followed for proposed model

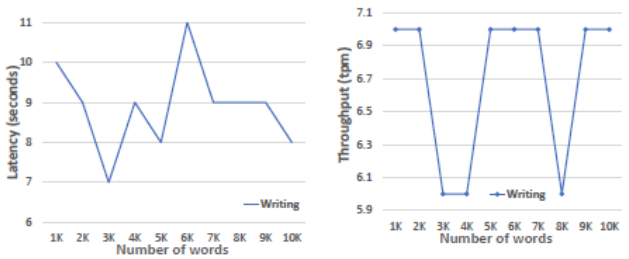
V. SYSTEM IMPLEMENTATION

MODULES

The implementation consists of two components: throughput analysis (TA) and latency analysis (LA). Without the imported modules, both of the modules are less than 5 KB in size. The LA module keeps track of how long it takes to write or list a message of various sizes. To be more specific, the LA module's functions include the ability to sample messages (such as customer reviews), track how long it takes to write or list messages on Hyperledger Fabric, and report on the total time required to process each message. The TA module is used to calculate how many times a message can be written or listed on Hyperledger Fabric every minute.

VI . RESULTS AND DISCUSSION

We investigated signature and verification performance in connection to the output results of the two assessment groups. Figure 6 depicts the latency and throughput of signing and verifying a 1,000-word message with varied key group lengths. It is clear that signing throughput ranges from 200 tps to 10 tps, whereas signing delays range from 5 ms to 80 ms for different key lengths. The time and throughput of signing are strongly impacted by the length of the keys. Shorter keys have lower latency than longer ones, but they can sign verification more continuously and with a better throughput when shorter keys are used. By comparison, we can see that the verification throughput is around 600 tps, with a latency of less than 1 ms. As a result, the effects of different key lengths on verification delay and throughput are negligible.



(a) Latency of writing a review. (b) Throughput of writing a review.

Fig 2. Latency and throughput of writing a review having different word counts

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

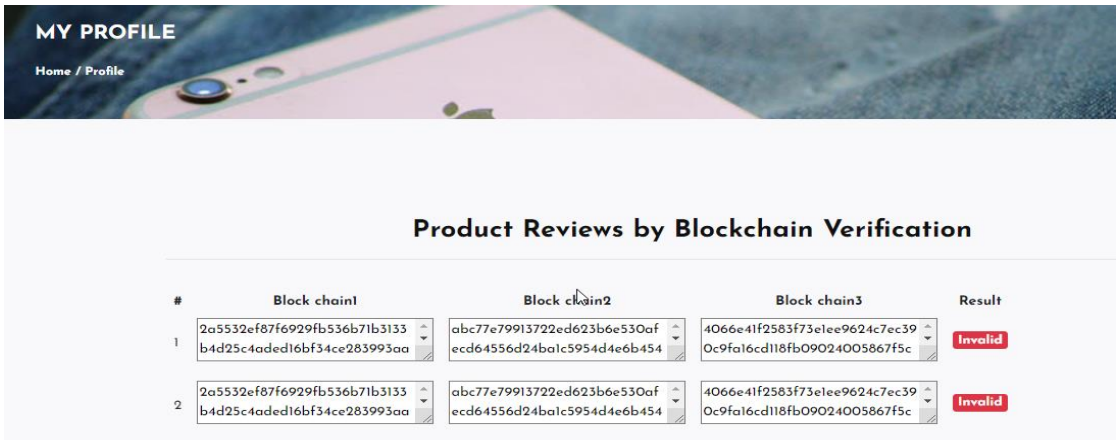


Fig 2. Blockchain based Customer Review Verification

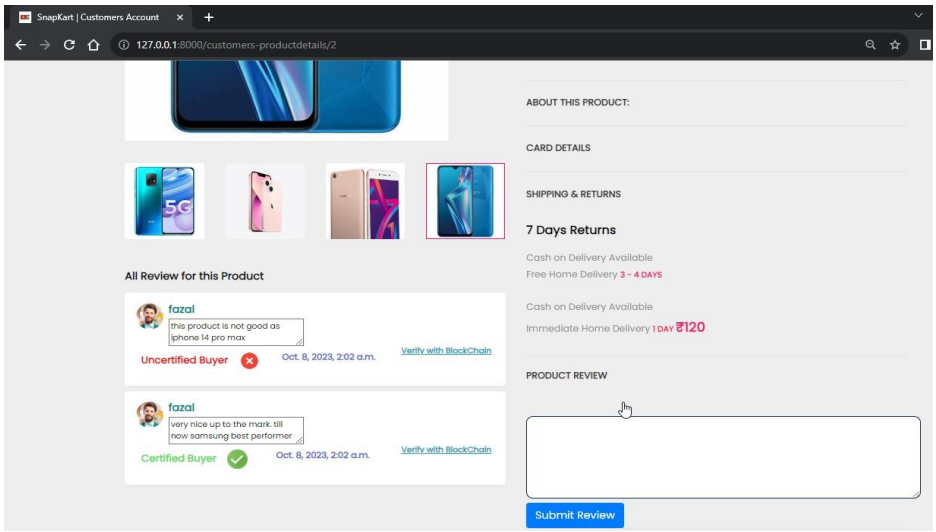


Fig 3. Showing Verified and Unverified Details

VI I.CONCLUSION AD FUTURE WORK

Customers can share their experiences by submitting reviews. We recommend RevBloc as a safe, effective, and user-friendly platform for client evaluations. RevBloc prevents manipulation by a single or small group of malicious actors by storing reviews on blockchain nodes owned by all participating organizations. We successfully implemented a RevBloc proof-of-concept prototype to demonstrate the practicality of our methodology. We plan to develop our solution in the future to make it more reliable. We would consider adding peer nodes for each business to increase the blockchain's processing power and storage capacity, allowing us to conduct a full inspection. As a result, the platform's availability and capacity may be enhanced.

REFERENCES :

[1] K. Test, "How to effectively use customer reviews in software marketing," https://www.gartner.com/en/digital-markets/insights/ how-to-effectively-use-customer-reviews-in-software-marketing, 2020.

ISSN: 2348-1358

Impact Factor: 6.901

NAAS Rating: 3.77

[2] B. Schneier and J. Kelsey, "Secure audit logs to support computer forensics," ACM TISSEC, vol. 2, no. 2, pp. 159–176, 1999.

[3] M. Bellare and B. Yee, "Forward-security in private-key cryptography," in Cryptographers' Track at the RSA Conference. Springer, 2003, pp. 1–18.

[4] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[5] J. L. Dautrich and C. V. Ravishankar, "Security limitations of using secret sharing for data outsourcing," in CODASPY. Springer, 2012, pp. 145–160.

[6] N. Li, "Research on Diffie-Hellman key exchange protocol," in 2010 2nd International Conference on Computer Engineering and Technology, vol. 4. IEEE, 2010, pp. V4–634.

[7] J. Kelsey, J. Callas, and A. Clemm, "Signed syslog messages," Request for Comment RFC, vol. 5848, 2007.

[8] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in Proceedingof 9th International Conference on Theory and Practice in Public-Key Cryptography, 2006, pp. 257–273.

[9] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 public key infrastructure certificate and CRL profile," RFC 2459, January, Tech. Rep., 1999.

[10] R. Accorsi, "A secure log architecture to support remote auditing," Mathematical and Computer Modelling, vol. 57, no. 7-8, pp. 1578–1591, 2013.

[11] J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," in ACM International Conference Proceeding Series, vol. 2, 2006, pp. 203–211.

[12] S. Zawoad, A. K. Dutta, and R. Hasan, "SecLaaS: Secure logging-as-aservice for cloud forensics," in ACM ASIA CCS, 2013, pp. 219–230.

[13] M. M. Ahsan, A. W. A. Wahab, M. Y. I. Idris, S. Khan, E. Bachura, and K.-K. R. Choo, "CLASS: Cloud log assuring soundness and secrecy scheme for cloud forensics," IEEE Transactions on Sustainable Computing, 2018.

[14] T. Kunz, A. Selzer, and U. Waldmann, "Automatic data protection certificates for cloud-services based on secure logging," in TCC. Springer, 2014, pp. 59–75.

[15] Y. Yu, L. Xue, M. H. Au, W. Susilo, J. Ni, Y. Zhang, A. V. Vasilakos, and J. Shen, "Cloud data integrity checking with an identity-based auditing mechanism from RSA," FGCS, vol. 62, pp. 85–91, 2016.

[16] A. A. Yavuz and P. Ning, "BAF: An efficient publicly verifiable secure audit logging scheme for distributed systems," in ACSAC. IEEE, 2009, pp. 219–228.

[17] B. Putz, F. Menges, and G. Pernul, "A secure and auditable logging infrastructure based on a permissioned blockchain," Computers & Security, vol. 87, p. 101602, 2019.

[18] L. Shekhtman and E. Waisbard, "EngraveChain: Tamper-proof distributed log system," in Proceedings of the 2nd Workshop on Blockchainenabled Networked Sensor, 2019, pp. 8–14.