A CRYPTOGRAPHIC APPROACH TO PRIVACY PRESERVING DISCOUNT TICKET DISTRIBUTION

Dr.T.Amalrajvictoire[1*], M.Vasuki[2],J.Mugundhan[3]
[1]Associate Professor, Department of MCA, Sri Manakula Vinayagar Engineering College, Puducherry-605107,India.
[2]Associate Professor, Department of MCA, Sri Manakula Vinayagar Engineering College,Puducherry-605107, India.
[3]PGStudent, Department of MCA, SriManakula Vinayaga rEngineering College, Puducherry-605107, India.
amalrajvictoire@gmail.com[1],dheshna@gmail.com[2],mugundhan121001@gmail.com[3]

ABSTRACT

In regular ticketing systems, people who want discounts—like students, seniors, or those with disabilities—often need to show their IDs, which means revealing personal information. This can increase privacy concern and makes people at risk of identity theft. To fix this, This paper presents a system that keeps privacy in mind while handing discount tickets. The system allows users to prove they are eligible for discounts without sharing their personal information. A trusted third party (TTP) will confirm their eligibility and provides a secure, anonymous digital credential by attribute-based authentication, using JSONWeb Tokens(JWT). Additionally, usersin thegeneral category, who are not eligible for discounts, can also purchase tickets while keeping their identity private, ensuring inclusivity and privacy for all users. Ticket sellers will use these credentials to verify their eligibility, without seeing their private data. The system also stops problems like ticket resale, duplication, and fraud with secure ticket validation and cryptographic checks. I built this project using the MERN stack (MongoDB, Express.js, React, and Node.js), and this was tested to make sure it works well, keeps data private, and prevents fraud. In the end of this project , the system keeps personal information securely while ensuring tickets are valid and authentic. It's a great fit for public transport, events, and online services, offering a solid solution that balances privacy and security.

KEYWORDS: Privacy-Preserving Ticketing, Attribute-Based Credentials, Cryptographic Authentication, Discount Verification System, Trusted Third Party (TTP), JSON Web Token (JWT)

1. INTRODUCTION

Most of the public services like as transportation, museums, and events discounted tickets are offered to some of the groups like students, senior citizens, or individuals with disabilities. Traditionally, users need to provide official identification to access these benefits, often revealing their sensitive personal information such as age, name, or medical status. While this method helps confirm someone is eligible, it also creates serious risk to their privacy, including the possibility of someone stealing their identity or using their data incorrectly. One of the main challenges in such systems is achieving a balance between verifyinga user's eligibility and protecting their personal data. Existing methods are not only intrusive but also prone to fraud, such as fake ID usage, ticket resale, or ticket duplication. Furthermore, once a ticket is issued, there is little control over whether it is used more than once or transferred to another person. This paper proposes a privacy-preserving electronic ticketing system that uses cryptographic techniques to solve these issues. By leveraging attribute-based authentication and JSON Web Tokens (JWT), users can prove they are eligible for discounts without disclosing their actual identity. A Trusted Third Party (TTP) validates user attributes and issues anonymous digital

credentials. These credentials can be verified by ticket issuers without accessing any private user data. The system also includes mechanisms to prevent ticket duplication and double usage. The proposed system is built using the MERN stack (Mongo DB, Express.js, React, and Node.js) and demonstrates strong potential for real-world applications.

This paper discusses related work, details the system architecture and methodology, presents implementation results, and concludes with future improvement directions.

2. RELATEDWORK:

Electronic ticketing systems have, however, matured to adopt several privacy-protecting mechanisms. Conventional systems are based on identity authentication using physical or virtual ID cards, revealing sensitive user information like age, name, or disability. Even though credible in checking entitlement, such methods sacrifice user privacy. New technology has brought about digital signatures, secure QR codes, and even biometrics to prevent forgery and duplication threats. But these are still lacking in providing total anonymity upon verification.

Mut-Puigserver extensively surveyed electronic ticketing schemes and categorized them according to functionality (e.g., portability, expiration) and security attributes like anonymity, unlinkability, fairness, and non-overspending. Ticketing schemes were thenwidely classified into transferable, non-transferable, multi-use, and single-use schemes. The system presented in the current paper is a non-transferable, single-use scheme providing privacy attributes like unlinkability, anonymity, and prevention from fraud, which are usually missing in conventional systems.

Some privacy-friendly techniques have been suggested based on blind signatures. For example, Chaum suggested the original blind signature scheme adopted in subsequent research like Fan and Lei ufor e- voting and Song and Korba for pay-TV ticketing. These techniques allow users to obtain tickets without revealing contents to issuers. They fail to facilitate attribute-based authentication or selective disclosure, though, restricting their value in discount-ticketing applications.

Group signature-based schemes have been used to maintain anonymity with a provision for there vocation of anonymity by a trusted authority in the event of abuse. Nakanishi and Vives-Guasch used group signatures to implement electronic coupons and fare collection systems. Although they ensure unlink ability as well as revocable anonymity, these systems do not enable fine-grained, privacy-preserving attribute checks.

A better category is anonymous credential-based systems, in which users are able to establish eligibility without disclosing identity. Camenisch and Lysyanskaya's system and IBM's Idemix are leading in this category. Heydt-Benjamin combined anonymous credentials with NFC and e-cash for public transport systems. Arfaoui optimized the verification of credentials to enhance efficiency in mobile ticketing. But these approaches are normally too sophisticated for lightweight, web-based implementations.

Pseudonym-based schemes have been considered as well. Vives-Guasch proposed e-tickets based on pseudonyms with unlink ability and excludability. Although pseudonyms provide some degree of anonymity, they do not provide formal security proofs and donot include eattribute-based authorization.

The rest of the works depend on specific hardware or trusted devices, like TPMs, AIKs, and Personal Trusted Devices (PTDs) which restrict usability due to hardware dependence.

Notwithstanding the progress made in these categories, there are very few systems that incorporate privacy- preserving attribute-based access control in web-based or mobile electronic ticketing systems. Currentschemes typically do not balance anonymity, usability, scalability, and deployability on contemporary stacks.

This paper fills that gap by proposing a realistic, web- focused e-ticketing system that relies on JWT-based anonymous credentials delivered through a Trusted Third Party. In contrast to previous works, it uses the MERN stack for guaranteeing accessibility, extensibility, and ease of integration into real-world transit or event-based deployments. It accommodates attribute-based eligibility checks without exposing identity, guarantees unlinkability, ticket non- transferability, and double-spending

prevention—thus offering a major improvement over current models.

3. METHODOLOGY

Current Methodologies: Current electronic ticketing systems always depend on centralized identity authentication and access control processes. Conventional ticketing processes usually involve the production of government IDs or electronic identity credentials as proof of eligibility to receive concession tickets. Operationally sufficient, complete openness is made to the users' privacy regarding disclosure of personal attributes such as name, age, disability status, or membership.

A number of systems in use have utilized secure QR codes, digital certificates, and biometric authentication to provide more secure tickets against forgery or duplication. All these systems are based on identity- linked verifications, which provide very little protection against privacyinvasions. Anonymous credential systems like IBM's Idemix and Microsoft's U-Prove provide stronger protection of privacy through proving eligibility without showing identity. These systems are theoretically secure but generally too expensive or complicated for light- weight, web-based deployment environments. In addition, most of these schemes don't support selective disclosure, double-spendingprevention,or fine-grained attribute-based access.

Current deployments miss the inclusion of privacy- friendly mechanisms in wide-range applications suchas MERN (MongoDB, Express.js, React.js, Node.js), and deployable, scalable, and privacy-enriched solutions are needed for publicly available e-ticket systems.

Proposed Methodology: The system in this submission is a privacy-aware attribute-based anonymous credential-based lightweight electronic ticketing system. Users are enabled to acquire and present cryptographically signed credentials attesting to eligibility—age, disability, or student—and conceal personal identity. The system is developed solely onthe MERN stack to yield real-time, seamless performance for web and mobile applications.

Attribute-Based Credential Issuance: A Trust Third Party (TTP) verifies user-supplied data and issues a digitally signed JSON Web Token (JWT) with eligibility attributes, not identity information.

Anonymous Proof Presentation: Users present the token to vendors when buying tickets. Sellerscheckthe cryptographic signature and inlined attributes without retrieving identity, allowing unlinkability and anonymity.

Double-Spending Detection: Token state is not only recorded in the backend logs but also accompanied by timestamps. Reuse of a token is labeled and blocked in realtime.

Role-Based Access Control: Every user type—such as normal users, TTPs, vendors, and verifiers—is assigned their own view and permissions. Access is securely handled by secure API paths.

End-to-End Encryption: Everything transmitted across the internet is secured using HTTPS. Sensitive information, such as TTP user data, is stored securely and accessible to only those with appropriate access The system accommodates numerous use cases suchas:

Public Transit & Mobility Services: Affiliation-, disability-, or age-competitive fare for buses, trains,andride-shares.

Digital Service Tokens: One-time credentials for print/download services where user attributes control entitlement.

Event Ticketing: Membership-, affiliation-, or other attribute-based entry to concerts, conferences, and tourist destinations.

Coupling attribute-based authorization, anonymous credentials, and MERN-based deployment, the suggested methodology provides areal-world,scalable, and privacy-preserving solution in contrast to standard electronic ticketing systems.

4. DATADESCRIPTION

To determine who receives a discount, the system considers some facts about the user—such as whether they're a student, senior citizen, or have animpairment. The facts serve to verify whether somebody qualifies. Yet the system never discloses or displays personal information such as the individual's entire name, age, or precise impairment. It all remains private while

still ensuring the correct people receive the discount.

The data for the system is divided into two categories:

User Attributes: These are whether a user isa student, senior citizen, or disabled. These are authenticated by a Trusted Third Party (TTP) and then an anonymous digital credential is issued to the user once they are found to be eligible.

Ticketing Transactions: When a user requests for the ticket, their eligibility is checked by the ticket provider, and then the system records which discount has been used like, student discount or senior citizen discount. This traces the usage of the ticket but does not have any personal identifiable information.

Preprocessing: Before processing all the data, all personally identifiable information (PII) is removed. For example, only the fact that a user is eligible for a student discount is sent to the system, but no studentID or other personal data sent to the system . The credentials issued by TTP are securely encrypted and released as JSON Web Tokens (JWTs) so that they can be easily consumed inside the ticketing system**.**

5. MODELARCHITECTURE

The architecture of the system combines cryptographic methods with scalable web technology. The purpose is to verify the eligibility of a user for discounts without revealing confidential personal information, while providing security, efficiency, and fraud control.

Attribute-Based Authentication: The Trusted Third Party (TTP) verifies the user's eligibility based on attributes (e.g., student or senior citizen). Having verified, the TTP produces a digitally signed digital credential. The credential contains only the credentials needed to verify eligibility and leaves nothing else discloseable about the user.

JSON Web Tokens (JWTs): After the Trusted Third Party (TTP) checks and confirms that the user is eligible for a discount, it creates a JWT (JSON Web Token). This token includes only the needed information and is sent securely to the ticketing system. JWTs are small and fast, they safely carry the discount details without sharing the users personal info like the user's name or age.

Cryptographic Signature: To stop people from copying or selling tickets, each ticket is protected with a special digital signature. The signature ensures nobody can alter or replicate the ticket. Subsequently, the system verifies whether the ticket is genuine or not.

Secure Ticket Validation: When a person uses this ticket, the system verifies that the JWT and the digital signature to ensure everything is correct or not. It verifies the ticket has not been altered or used in any incorrect manner. This prevents cheating, such as using the same ticket twice or selling it to an other person that who are not eligible for discounts

Architecture Diagram

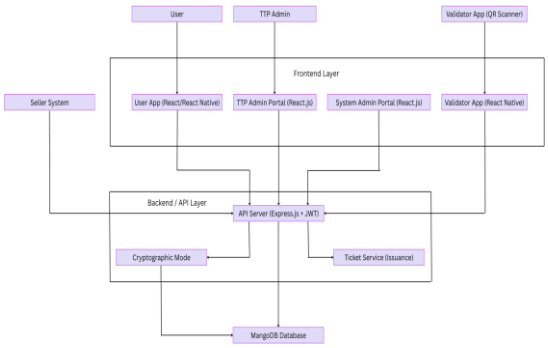
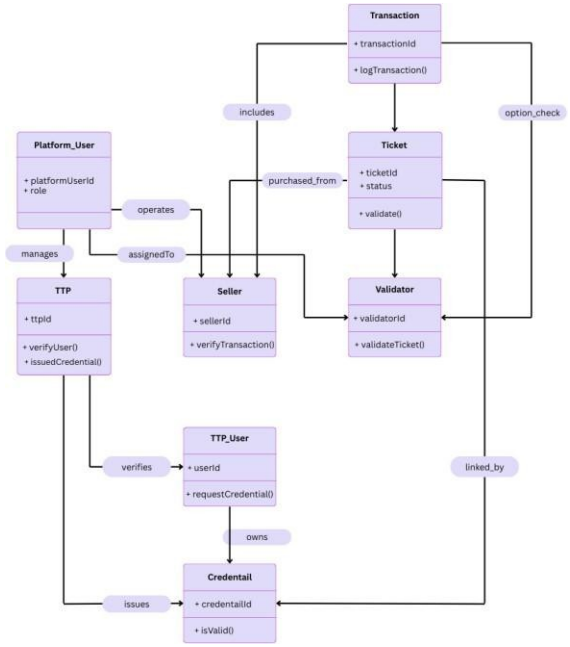


Fig1.SystemArchitecture

CLASS DIAGRAM



.

Fig2.Class Diagram of Ticketing System

6.DEALING WITH CLASS IMBALANCE

Occasionally in the systems, one of the people in a group receives more advantages than others. This is referred to as class imbalance. In our ticket system, this may occur if, say, students or elderly people receive more tickets than other groups, ori fan individual attempts to cheat the system by pretending to be part of a specific group. To address this, our system includes the following techniques:

Balanced Data Collection: We ensured that the data which is utilized to construct and validate the system has an equal number of users from all groups (such as students, seniors, etc.). This enables the system to treat all users equally and not favor any particular group.

Fraud Detection: How people use tickets was monitored by the system. If it observes something unusual like one group demanding a lot of tickets than ever before it marks that case to verify. It prevents people from cheating.

Making Sample Data: For those groups with fewer users (such as people with disabilities), we generate additional sample data to ensure that they are included fairly. This allows the system to work for everyone, even the smaller groups.

7. EVALUATION METRICS

To measure how well our privacy-focused ticketing system works, we looked at some of the most important features:

Privacy Protection: We made sure that the system keeps the personal information private of the users . It must be able to tell if someone is qualified for a discount without exposing their personal information like their name or their age. We also tested to ensure that no one can hack the systems or get sensitive information. All these were tested to ensure they meet privacy laws like GDPR.

Fraud prevention: We tested the system to prevent cheating—i.e., duplicating tickets, selling tickets to another individual, or trying to use the same ticket over and over again. We created different simulated scenarios to see how the system would respond, and it was able to catch and block these moves.

User friendliness: The system was designed as simple as possible to be used by everyone. The users should be able to confirm their entitlement and book tickets without being confused. We gathered user feed backand observed how easily they were able to navigate every step.

Speed and Performance: We tested how fast the system runs when generating and checking tickets. We also tested how it works under heavy load—like lots of people doing it at the same time—so that it stays fast and does not crash or become slow.

Security Checks: We carefully tested the tools that protect the system, like digital signatures and JWTs. Our goal was to find any weak points that hackers could take advantage of and fix them before they became a risk

8.EXPERIMENTAL RESULTS AND ANALYSIS

Functional Verification: The system was thoroughly tested to confirm that all functionality requirements were satisfied across various user roles such as users, trusted third parties (TTPs), ticket sellers, and validators. The credential issuance process worked as expected, allowing users to request verification and get digital credentials based on successfully verified eligibility. Ticket purchase transactions, such as anonymous proofs and eligibility verification, were executed effectively without disclosing identities. Role-based access control mechanisms provided for the specific actions within the system to be taken by only authorized users.

Performance Evaluation: Load testing showed thatthe system could support as many as 350 simultaneous ticket validation requests per second, and with an average response time of 180 milliseconds per validation. Cryptographic processes like JWT signature verification and anonymous proof verification acquired zero extra overhead due to effective backend design and usage of the optimal libraries. Ticketing issuance that connected with the credential verification and the ticket building took an average with less than 500 milliseconds per request. We tested the system by simulating 1,000 transactions per minute, and it stayed fast and responsive the whole time.

Security and Privacy: Security testing proved that resistant to common web-based attacks like injection attacks, cross-site scripting (XSS), and unauthorized access. Penetration testing proved that two low-level vulnerabilities, which were fixed a tbefore deployment. Credential and the ticket forgery attempts to failed because of the utilization of digitally signed tokens. The system also regularly detected and prevented double-spending attempts through secure backend verification logic and transactional recording.

Privacy analysis showed that efforts to correlate anonymous tickets or credentials with user identities failed, as with un link ability promises of the system's crypto design. Individual user properties were safely stored in hidden backend stores with access control in place and encryption, and communication was safely masked with HTTPS. Compared with traditional systems, privacy breaches and data exposure were much less likely to happen.

Reliability and Data Consistency: We tested how the system handles failures, and it kept running smoothly with almost no issues, thanks to backup systems and copied databases. Even when many users were using it at the same time, it tracked ticket use and transactions correctly, without messing up any data.

Usability: User testing across multiple system roles provided very positive feedback. Users found the interface intuitive and credential request and ticketing workflow easy to navigate. Ticket validators compliment edtherapid scanning and convenient isual feedback regarding ticket validity and eligibility type. Most importantly, users cited being able to access services without exposing personal identity as a key advantage, underscoring the system's success in achieving usability at the expense of privacy.

9. CONCLUSION:

This paper proposed the design, development, and analysis of an attribute-based anonymous credential-based privacy-preserving Electronic Ticketing System. The system effectively addresses the privacy concerns embodied in traditional identity-based ticketing systems by decoupling user eligibility from identity verification. Through the inclusion of a Trusted Third Party (TTP) for the authentication of attributes and use of JWT-based cryptographically signed credentials, users are able to anonymously and securely use discounted ticketing services.

The system, developed using the MERN stack, offers modular, scalable, and maintainable architecture for real-world deployment. The system offers a new array of combinations of cryptographic privacy-preserving technologies in a web-based state-of-the-art environment. Experimental evaluation guaranteed the functional correctness, real-time execution, and resilience against fraud, leakage of data, and abuse of credentials of the system.

In conclusion, this paper demonstrates that privacy- preserving authentication protocols can effectively be employed in practical digital ticketing systems. It provides a basis for future systems to pay attention to user privacy, security, and trust in public services.

Future Improvements: In the future, a number ofcore areas provide potential to develop this privacy- enhancing ticketing platform further. Our current activity and future direction is aimed at enhancing the platform to become more accessible, flexible, and robust, always with a strong focus on maintaining privacy and security requirements. Possible enhancements include:

Decentralizing Trust for Issuance of Credentials: The system at present is dependent on discrete Trusted Third Parties. A fascinating direction is to explore a
More decentralized trust modelin volving block chain or distributed ledger technology. This would improves reliability, enhances calability, and expand the range of is users supported beyond discrete parties.

Improving Attribute Confirmation Features: To improve more of an extensive set of discount scenarios, we intend to incorporate more complex attribute tests. This means advancing towards verifying complex specifications, such as age ranges or discrete sets of attributes (e.g., "student at X university,""veteran resident of Y region"), so that ticket sellers can enforce more specific discount rules.

Offline Validation Support: Internet might not always be available where tickets are checked. Allows devices to validate tickets offline using secure methods would make sure checks still work. Later, the data can be synced when the net work is available."

Integration with Digital Wallet : To make the things more suitable, we allow users in future to save their tickets to phone wallets like Google Wallet or Apple Wallet. This would make showing the ticket when needed much simpler

Building Native Mobile Experiences: We plan to create mobile apps for users and ticket checkers. These apps would be made for phones like Android and iPhone to work faster, users feel smoother, and use the phone features to keep things more secure.

Automating Attribute Verification Procedures: Accelerating the process of issuing credentials may be done by linking the system with vetted external digital identity or attribute sources. Where possible and legal, this would automate some procedure of attribute verification that now needs TTP administrators' manual review.

All these intended developments have the purpose of broadening the outreach and value of the system, andof improving the experience for all parties involved, while inherently strengthening its fundamental privacy and security assurances.

10. REFERENCES

[1] Mut-Puigserver,M.,Payeras Capellà,M.,andRifà- Pous, H., “A survey of electronic ticketing applied to transport,” Computers & Security, vol. 37, pp. 103– 121, 2013.

[2] Fan, K., and Lei, X., “A blind signature scheme based on quadratic residues,” Electronics Letters, vol. 32, no. 13, pp. 1212–1213, 1996.

[3] Milutinović, M., and Varadharajan, V., “MOTET: Mobile Transactionsusing Electronic Tickets,”inProc. 19th Int. Conf. Advanced Information Networking and Applications (AINA'05), pp. 427–432, 2005.

[4] Heydt-Benjamin, T. S., Defrawy, K. E., and Juels, A., “Privacy for public transportation,” in Proc. 6th Workshop on Privacy Enhancing Technologies (PET'06), pp. 1–19, 2006.

[5] Song, R., and Korba, L., “Pay-TV system with strong privacy and non-repudiation protection,” inProc. 14th Int. Workshop on Database and Expert Systems Applications (DEXA'03), pp. 362–366, 2003.

[6] Gudymenko, I., “A privacy-preserving e-ticketing system for public transportation supporting fine- granular billing and local validation,” in Proc. 5thACM Conf. Data and Application Securityand Privacy (CODASPY'15), pp. 27–34, 2014.

[7] Kerschbaum, F., and Schropfer, A., “Privacy- preserving billing for e-ticketing systems in public transportation,” in Proc. 2013 ACM Workshop on Privacy in the Electronic Society (WPES'13), pp. 143– 154, 2013.

[8] Rupp, A.,Hinterwälder,G.,Baldimtsi, F.,and Paar, C., “P4R: Privacy-preserving pre-payments with refunds for transportation systems,” in Financial Cryptography and Data Security, pp. 205–221, Springer, 2013.

[9] Vives-Guasch, A., and Rifà-Pous, H., “A secure automatic fare collection system for time-based or distance-based services with revocable anonymity for users,” in Proc. 2012 ACM Symposium on Applied Computing (SAC'12), pp. 1453–1458, 2012.

[10] Chaum, D., “Blind signatures for untraceable payments,” in Advances in Cryptology, pp. 199–203, Springer, 1983.

[11] Boneh, D., Boyen, X., and Shacham, H., “Short group signatures,” in Advances in Cryptology – CRYPTO 2004, pp. 41–55, Springer, 2004.

[12] Camenisch, J., and Lysyanskaya, A., “An efficient system for non-transferable anonymous credentialswith optional anonymity revocation,” in Advances in Cryptology–EUROCRYPT2001,pp.93–118, Springer,2001.

[13] Fujimura, K., and Nakajima,Y.,"General-purpose digital ticket framework," in Proc. 3rd USENIX Workshop on Electronic Commerce, pp. 155–166,1998.

[14] Quercia, D., and Hailes, S., "MOTET: Mobile Transactions using Electronic Tickets," in Proc. 2007 ACM Workshop on Privacy in the Electronic Society (WPES'07), pp. 91–98, 2007.

[15] Boneh, D., Lynn, B., and Shacham, H., "Short signatures from the Weil pairing," in Advances in Cryptology–ASIACRYPT2001,pp.514–532, Springer,2001.

[16] Abe, M., and Okamoto, T., "Provably secure partially blind signatures," in Advances in Cryptology– CRYPTO'99, pp. 271–286, Springer, 1999.

[17] Pedersen, T.P., "Non-interactive and information- theoretic secure verifiable secret sharing," in Advances in Cryptology – CRYPTO'91, pp. 129–140, Springer, 1991.

[18] Nakanishi, T., Fujii, H., Hira, Y., and Funabiki,N., "Revocable group signature schemes with constant costs for signing and verifying," IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, vol. E92.A, no. 1, pp. 136–147, 2009.

[19] Jorns, O., and Kuntze, N., "Trusted ticket systems and applications," in Proc. 22nd IFIP Int. Information Security Conf. (SEC'07), pp. 145–156, Springer, 2007.