**Aithabatula siddhardha**
computer science and systems engineering,
Andhra University college of engineering ,
visakhapatnam,india

**Dr. kondapalli venkata ramana**
Associate Professor
computer science and systems engineering,
Andhra University college of engineering ,
visakhapatnam,india

# Privacy-Preserving Electronic Ticket Scheme withAttribute-based Credentials

**Abstract :** E-tickets, which are electronic replicas of paper tickets, allow customers to access desired services more easily and efficiently. However, users of e-tickets can have privacy concerns. In order to safeguard users' privacy and make ticketing based on a user's traits easier, a privacy-preserving electronic ticket scheme with attribute-based credentials is proposed in this work. Our suggested plan contributes the following: Users can purchase different tickets from ticket sellers without disclosing their exact attributes; Two tickets belonging to the same user cannot be linked; A ticket cannot be transferred to another user; A ticket cannot be used twice The proposed scheme's security is formally proven and reduced to a well-known (q-strong Diffie-Hellman) complexity assumption; and The proposed scheme is implemented. The plan has been put into action, and its effectiveness has been objectively assessed. We believe that our attribute-based, privacy-preserving e-ticket system is the first to offer these five advantages. In order to purchase cheap event or transportation tickets, users must persuade ticket vendors that their characteristics (such as age, career, and location) comply with the ticket price restrictions. More broadly, any system where a user's attributes (or entitlements), rather than their identities, determine access to services can use our scheme.

**Index Term: -** Anonymity, Attribute-based Credentials, Privacy-enhanced Authentication

## I Introduction

Electronic ticket (e-ticket) systems have received a lot of attention from both the business community [1]–[3] and the academic research communities [4]–[6] because of their mobility and flexibility. Because they can cut paper expenses (tickets can be saved on a hand-held device), e-tickets are appealing to both transport operators and passengers (tickets can be purchased and delivered any time and anywhere). Due to the potential to link various e-ticket transactions to a specific user—in contrast to anonymous paper-based tickets—and thereby potentially reveal private information, such as working habits, likely places of employment, etc.—the use of e-tickets also raises many concerns about the privacy of its users.

Designing e-ticket systems that protect client privacy and are also formally proven to be secure is therefore a crucial topic of research. Many privacy-preserving e-ticket schemes have used anonymous authentication, which enables users to authenticate without disclosing their identities, to safeguard a user's privacy [4], [7]- [11]. Many of these techniques, though, have not been properly shown to be secure. The exceptions put up by Arfaoui et al. [8] and Rupp et al. [12] stand out. Arfaoui et al[8] .'s explicit definition of their e-ticket security models, which includes unforgetability, Unlinkability and non-repudiation were also claimed, although the authors only offered a very cursory justification. Rupp et al[12] .'s privacy-preserving pre-payments with refunds techniques were formalised, and they included transportation authority security and user privacy, but their scheme's security proof was once more at a high level. Support for different tickets based on a user's

characteristics (such as age, location, handicap, career, etc.), i.e., to offer discounts for, say, students or disabled passengers, is another criterion of a realistic e-ticket system. However, there is a chance that such a ticket system could reveal more personal data about a user than necessary when buying or validating tickets if it is not done appropriately. For instance, a student purchasing a ticket at a reduced price for students can wind up disclosing the university at which She is enrolled, and depending on the student card, she may

even be a student by birth, but neither of these factors affect whether she can get the student discount. She must be able to show that she is a legitimate student as the bare minimal proof. Similar to this, a passenger with a disability can be required to disclose more information about it to the ticket issuer or verifier than is required for buying or verifying a ticket. This problem was addressed by Gudymenko [10] and Kerschbaum et al. [11], but their plans were not fully demonstrated.

Transport companies are understandably concerned about the fraudulent use of e-tickets given how simple it is to copy them. Therefore, another crucial function that an electronic ticketing system should enable is double spend or, more broadly, overspend detection, which is the process of evaluating if a ticket has been used excessively.

**2 Literature survey**

Mut-Puigserver et al. [5] surveyed numerous e-ticket systems and summarised their various functional requirements (e.g. expiry date, portability, flexibility, etc.) and security requirements (e.g. integrity, authentication, fairness, nonoverspending, anonymity, transferability, unlinkability, etc.). E-ticket schemes are classified into different types: transferable tickets [6], [7], untransferable tickets [4], [14], multiuse tickets [4], [5] and single-use tickets [4], [6], [7], [15]. Our scheme falls into the untransferable, single-use tickets categories while providing anonymity, unlinkability, nonoverspending and flexibility.

We now assess how our plan stacks up against a variety of different plans. To safeguard user privacy, these methods used blind signatures [16], group signatures [17], anonymous credentials [18], and pseudonyms [17], [19]. Blind Signatures' E-Ticket Schemes. A user can obtain a signature on a message using a blind signing mechanism without the signer being aware of the message's content. Fan and Lei [20] proposed an electronic ticket voting method based on Chaum's blind signature proposal, which would allow each voter to cast one ballot for multiple elections.

**3 Formual definitions :**

Our scheme consists of the following four realities central authority CA, stoner U, ticket dealer S and ticket verifierV. • CA authenticates U and S, and issues anonymous cre dentials to them; • S registers to the CA, obtains anonymous credentials from the CA, and sells tickets to U in agreement with the ticket programs; • U registers to the CA, obtains anonymous credentials from the CA, purchases tickets from S, and proves the possession of tickets to V; • V validates the tickets handed by U and detects whether a ticket is double spent. The relations between the different realities in our scheme.

**Ticket Issuing**

This computation between U and S is completed naturally. A ticket is produced using information from U's secret public key pair, SKU;PKU, his credits AU, his certificate sU, a nom de plume , the ticket methods P, a true period VP, the chosen organisations Serv, and therefore the public limits params. TicketU. S inputs the user name, the ticket price, the ticket value, the real-time period (VP), the chosen organisations (Serv), the general public limitations parameters, and his secret public key pair (SKS;PKS) (PsU;Serv).

**Ticket Validating**

Parameters: U SKU Ps U Ticket U V VP Serv Serv Parameters for $ V! Serv TransT; 0=1 U and V made a wise decision in determining this. U information checks his secret public key pair SKU;PKU, his ticket TicketU, the significant periodVP, the chosen services Serv, and therefore the public boundaries params to see whether it is legitimate. U information returns 1 if TicketU is valid, but 0 if it's invalid. the general public border parameters, the chosen governmental Serv, and therefore the long-term VP are some sources of information. Serv;TransTÞ.

**Model of Security**

It is exceedingly challenging to develop a plan that can be used to offer UC security, despite the very fact that UC security models have some significant strengths. Nobody thinks that any of the creative tagging techniques now in use has been validated using the UC security model. We then describe the safety of our scheme using the reproduction-based .. The variance of the corresponding real-world and ideal-world assessments may be a defining feature of the reproduction-based approach. The experiment's actual

results. We first show how our approach functions within the scenario where the focus point CA, the ticket seller S, the customer U, and therefore the ticket verifier V are all reliable. a true foe has From SE, ID, S S uses CA to perform the seller enlistment computation SRegistration. S uses the command KG1'!SKS;PKS to make the result sS, passing in his personality IDS, the enigma public key pair SKS; PKS, and therefore the public boundary parameters. S's public key PKS, his lord secret key MSK, and the public boundaries parameters are used as inputs by CA to get S's character IDS and public key PKS. S sends a piece of knowledge (b 2f 0;1g) to E to let him know whether the SRegistation computation was successful or not. The client enrollment computation is handled by URegistration with CA in response to E's enrollment message "registration;ID U;AU." Using his character IDU as input, U runs KG1'!SKU;PKU and provides credits. The secret-public key's AU.pair "SKU;PKU," and therefore the public boundary parameters to produce a result.

**4 Implementation Study**

in the exsisting system they presented an electronic ticket method for voting in which each voter can cast one ballot for multiple elections. In order to maintain user privacy and offer non-repudiation in pay-TV systems, devised an e-ticket system. Chaum's blind signature system some of the authors suggested e-ticket plan to create both limited-use and unlimited-use tickets for mobile transactions. The privacy-preserving pre-payments with refunds techniques developed short signature schemes, signature approach to accomplish the privacy-preserving aggregation of refunds

In the existing work, the system did not implement Boneh-Boyen (BB) Signature which leads very less effective.This system is less performance due to the purpose of existing system is to ensure that a verifier can only ask for a ticket once to prevent an honest user from being de-anonymised by a malicious verifier

**4.1 Existing Methodlogy**

General-purpose programming languages (like C++, Java, or Python) and specific-purpose simulation languages (like Arena and GPSS) are the two methods used to create simulation tools (Leemis and Park, 2006). The latter has various built-in capabilities (such as statistics, an event scheduler, and animation) that shorten the time needed to construct models, while the former is more flexible and well-known. According to Leemis and Park (2006), there is disagreement and dispute over which approach is best. The use of general-purpose languages to create simulation models is made possible by simulation frameworks, which are also important to note.

**4.2 Proposed methdology**

In the proposed system, the system proposes a new privacy-preserving e-ticket scheme using attribute-based credentials which supports issuing different tickets depending on a user's attributes. Our scheme protects an honest user's privacy while allowing for the de-anonymisation of users who try to use their tickets more than once (double spend detection). It is also a general e-ticket system and can be used in various application scenarios including:

mobility as a service transport tickets (e.g. rail, bus, etc.) where age, disability, profession, affiliation, etc.might determine the prices of tickets

one-off token for Internet services (e.g. print service, download service for multimedia, etc.) where age, affiliation, membership might determine the service/accesslevel;

e-Voting where age, nationality, voting district, etc.might determine the voting ballot that should be issued;

event tickets (e.g. concert, tourist attractions, conferences, etc.) where age, affiliation, disability, etc.might determine the ticket price/access rights.

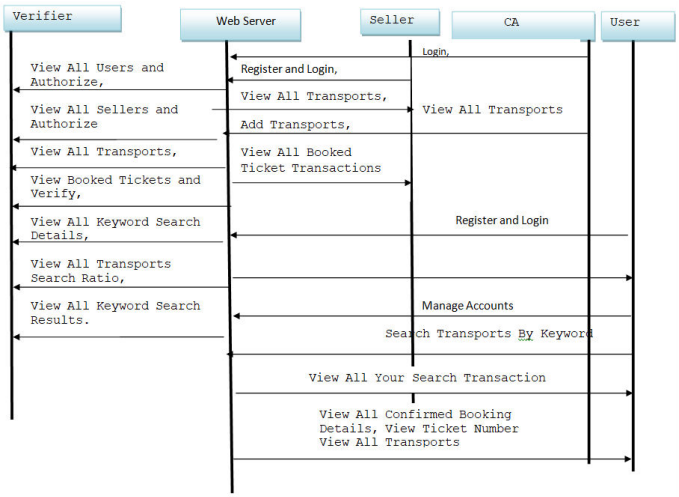


**Fig 1: Sequence Diagram**

### 4.2.1 Advantages of proposed method

(1) Attribute based Ticketing: users can buy different tickets depending

on their signed attributes without releasing their exact details;

(2) Unlinkability: two tickets of the same user cannot been

linked ;

(3) Untransferability: a ticket can only be used by the ticket holder and cannot be transferred to another user;

(4) Double Spend Detection: a ticket cannot be double spent and the identities of users who try can be revealed;

(5) Formal Security Proof: the security of the proposed scheme is formally proven and reduced to the well-know q-strong Diffie- Hellman complexity assumption.

(6) Performance Evaluation: the performance of our scheme has been measured on both Android and PC platforms.

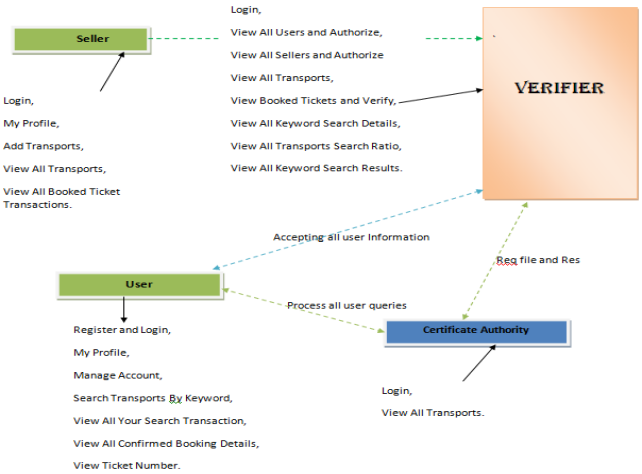


**Fig 2:- Architure Diagram**

### 4.3 Methodology and Alogrithams

#### 4.3.1Secure multiparty computation:

Llie, Brian, and Caroline use a secure multi-party computation protocol to calculate averages without revealing their private salary information in the process. Secure Multiparty Computation protocols utilize a well-established cryptographic concept called additional secret sharing, which refers to the partitioning of secrets and their distribution among a set of independent, willing participants.

#### 4.3.2 q-strong Diffie-Hellman:

Digital autographs are a central primitive in ultramodern cryptography. The security evidence of a hand scheme is generally grounded on a complexity supposition. The q-Strong Diffie- Hellman( q- SDH) supposition has come a common supposition used for a roster autographs. The q-SDH supposition was first defined by Boneh and Boyen in( 4). Roughly speaking, the q- SDH supposition in a bilinear group G of high order p states that it's intractable to cipher( c, g1/( a c)) for a freely chosen integer c ∈ Zp 1, where the input is g, ga, ga 2, • , ga q ∈ G. Although its time complexity is lower than standard hypotheticals( 8, 5), we can choose a larger group size to increase its time complexity. In this paper, we aren't interested in its time complexity but a comment made by Hohenberger and Waters( 16), who refocused out that the q- SDH supposition is less dependable than standard hypotheticals due to the number of correct answers. As the integer c can be freely chosen by the adversary from the space Zp, correct answers for a challenge input of the q- SDH supposition are exponentially numerous, while the correct answers for those standard hypotheticals have one only. For illustration, the only correct answer for the CDH supposition is g ab ∈ G for a challenge input g, ga, gb ∈G. Standard hypotheticals confining an adversary with one correct answer feel innately " harder " than the q- SDH supposition, which allows an adversary with a inflexibility to win.

#### 4.3.3 Central authority (CA)

It is the administrator of the whole system. Particularly, it sets up the system parameters for the access control implementation and View All Transports

CA publishes the ticket price polices $P = \{R_1, \cdots, R_{N_1}, S_1, \cdots, S_{N_2}\}$ where $R_i = [c_i, d_i]$ is a range policy (i.e. age, mileage) and $S_i = \{I_{i_1}, I_{i_2}, \cdots, I_{i_\zeta}\}$ is a set policy (i.e. location, profession, disbility) and consists of $\zeta$ items $I_{i_j}$ for $i = 1, 2, \cdots, N_1$ and $i = 1, 2, \cdots, N_2$.

CA runs $BG(1^\lambda) \rightarrow (e, p, G, G_T)$. Suppose that the longest interval length in $\{R_1, \cdots, R_{N_1}\}$ is $[0, q^k)$ where $q \in Z_p$ and $p > 2q^k + 1$. Let $g, g_1, g_2, g_3, \hat{g}_1, \hat{g}_2, \cdots, \hat{g}_{N_1}, \hat{h}, \hat{g}, \eta, \xi, \rho, \vartheta, \eta_1, \eta_2, \cdots, \eta_{N_2}$ be generators of $G$, $H : \{0,1\}^* \rightarrow Z_p$ and $H' : \{0,1\}^* \rightarrow G$ be two cryptographic hash functions.

CA selects $x, y, \mu_1, \mu_2, \cdots, \mu_{N_2} \xleftarrow{R} Z_p$ and computes $\hat{g} = g^x, \hat{h} = h^y, h_0 = h^{\frac{1}{x+\vartheta}}, h_1 = h^{\frac{1}{x+\vartheta^2}}, h_2 = h^{\frac{1}{x+\vartheta^3}}, \cdots, h_{q-1} = h^{\frac{1}{x+\vartheta^{q-1}}}, \tilde{h}_0 = h^y, \tilde{h}_1 = h^{y\vartheta}, \cdots, \tilde{h}_{q-1} = h^{y\vartheta^{q-1}}, \hat{\eta}_1 = \eta^{y_1}, \hat{\eta}_2 = \eta_2^{y_2}, \cdots, \hat{\eta}_{N_2} = \eta_{N_2}^{y_{N_2}}$ and $\left(\eta_1 = \eta^{\frac{1}{x+\vartheta\mu_1}}, \eta_2 = \eta^{\frac{1}{x+\vartheta\mu_2}}, \cdots, \eta_i = \eta^{\frac{1}{x+\vartheta\mu_i}}\right)_{i=1}^{N_2}$.

The secret key of CA is $MSK = (x, y, \mu_1, \mu_2, \cdots, \mu_{N_2})$ and the public parameters are $params = (e, p, G, G_T, g, g_0, g_1, g_2, \hat{g}_1, \hat{g}_2, \cdots, \hat{g}_{N_1}, \hat{h}, \hat{g}, \eta, \xi, \rho, \hat{g}, h_0, h_1, \cdots, h_{q-1}, \tilde{h}_0, \tilde{h}_1, \cdots, \tilde{h}_{q-1}, \eta_1, \eta_2, \cdots, \eta_{N_2}, \hat{\eta}_1, \hat{\eta}_2, \cdots, \hat{\eta}_{N_2}, (\eta_1, \eta_2, \cdots, \eta_i)_{i=1}^{N_2})$.

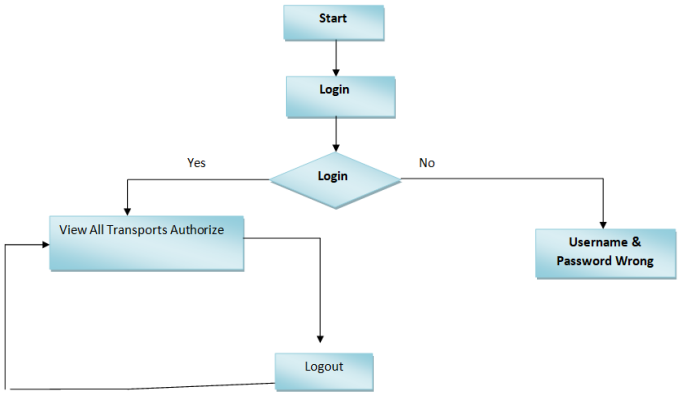


**Fig 3: Central authority (CA)**

#### 4.3.4 Verifier

He is the entity who outsources his/her data to cloud servers. To share his/her data with other intended entities, he/she defines access policies for data and performs the following operations like Login, View All Users and Authorize, View All Sellers and Authorize View All Transports, View Booked Tickets and Verify, View All Keyword Search Details, View All Transports Search Ratio, View All Keyword Search Results.

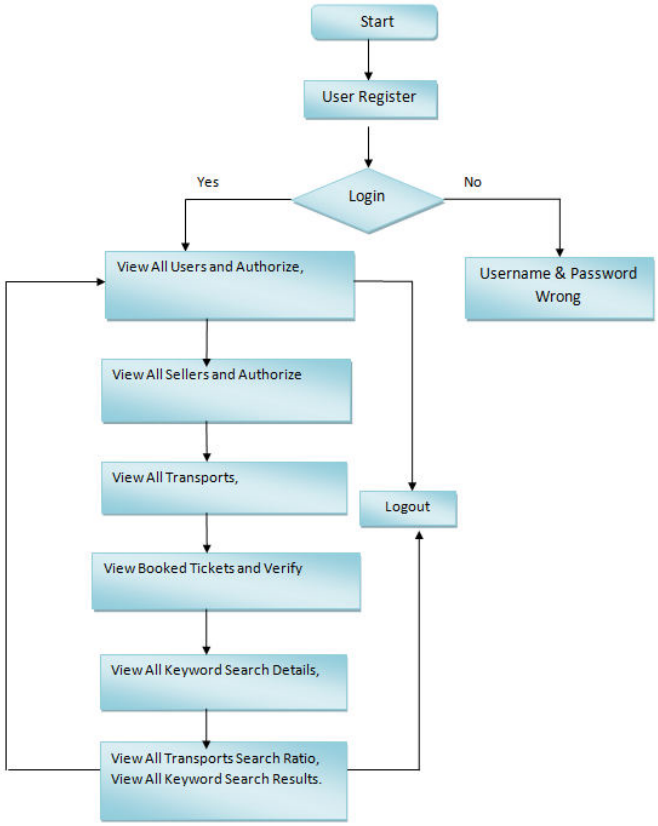


**Fig 4: verifier**

#### 4.3.5 Data consumer (User)

He is the entity who is interested in data contents. In our controlled collaborative access control scheme, each user is performing the following operations such as Register and Login, My Profile, Manage Account, Searc Transports By Keyword, View All Your Search Transaction, View All Confirmed Booking Details, View Ticket Number.

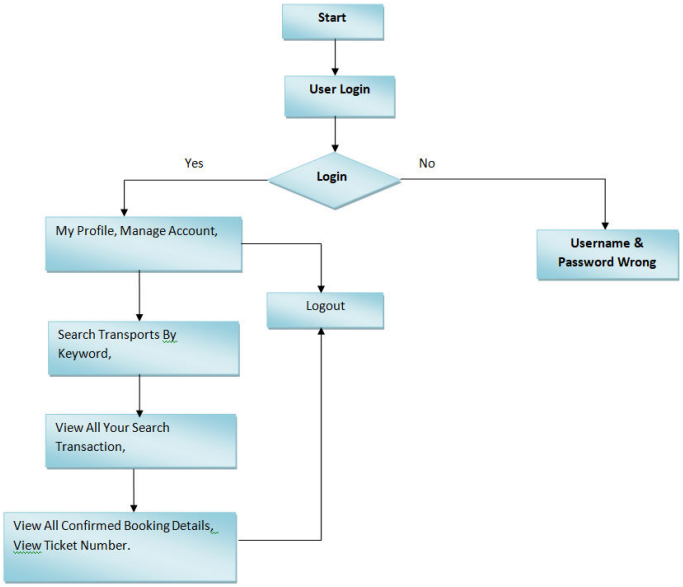


**Fig 5: Data consumer (User)**

### 4.3.6 Seller

The seller is the one who is selling the products via online and performs the following operations My Profile,Add Transports,View All Transports,View All Booked Ticket Transactions.

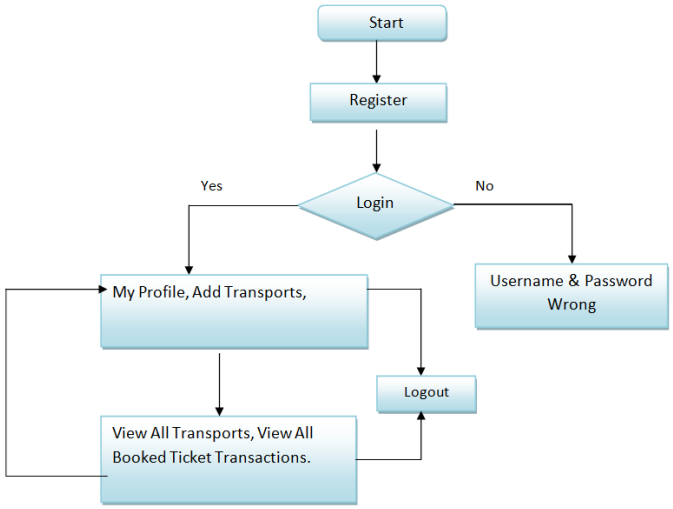


**Fig 6: seller**

### 4.3.7 Ticketing Alogritham

Our scheme consists of the following four entities: central authority CA, user U, ticket seller S and ticket verifier V.

- CA authenticates U and S, and issues anonymous credentials to them
- S registers to the CA, obtains anonymous credentials from the CA, and sells tickets to U in accordance with the ticket policies
- U registers to the CA, obtains anonymous credentials from the CA, purchases tickets from S, and proves the possession of tickets to V
- V validates the tickets provided by U and detects whether a ticket is double spent

### Results and Evolution Metrics

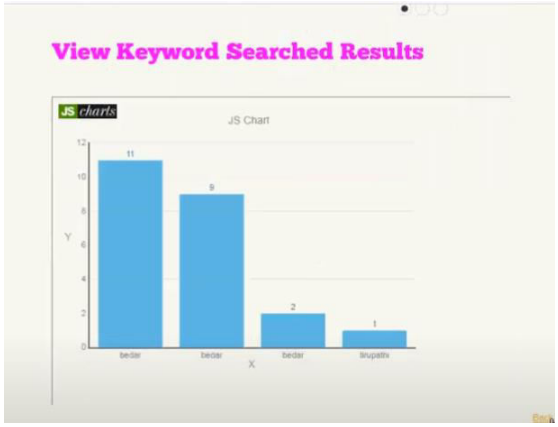


**Fig 7:- key word search graph by the consumer regarding vechile**

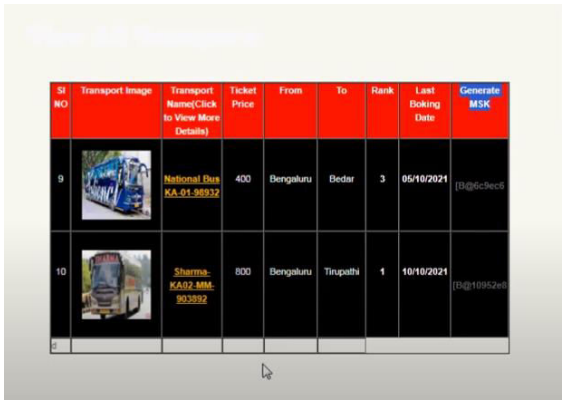


**Fig 8:- centeral authority who generates the master key for each vechile**


**Fig 9:- once the ticket is booked the verifier verifies the ticket and a signature is generated by the verifier**

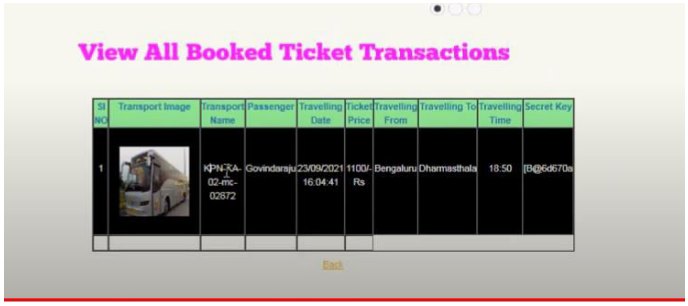


**Fig 10:- once ticket is booked a secret key is generated**

**5 Conclusion**

Several approaches have been put up to safeguard user privacy in e-ticketing, but they did not address attribute-based ticketing. In this paper, a method for implementing attribute-based ticketing was given, while maintaining user privacy. Our suggested plan contributes the following: (1) Users may purchase different tickets from ticket vendors without disclosing their precise characteristics; (2) Two tickets belonging to the same user cannot be linked; (3) A ticket may not be transferred to another user; (4) A ticket may not be used twice; (5) The security of the proposed scheme is formally proven and reduced to a well-known (q-strong Diffie-Hellman) complexity assumption; and (6) The scheme has been implemented and its effectiveness has been empirically evaluated. In the future, we'll examine how dynamic security models and proof are affected..

**6 References**

[1] United Airlines. (2017) Customer data privacy policy. [Online].
Available: https://www.united.com/web/en-US/content/privacy.aspx

[2] British Airways. (2004) British airways e-ticket for amadeus users. [Online].
Available:
http://www.britishairways.com/cms/b2b/tradeOnline/
nPacific/content/news and promotions/eticket amadeusn prompt.pdf

[3] Rail Delivery Group. (2017) Rail technical strategy capability delivery
plan. [Online]. Available: https://www.rssb.co.uk/rts/Documents/
2017-01-27-rail-technical-strategy-capability-delivery-plan-brochure.
pdf

[4] M. Milutinovic, K. Decroix, V. Naessens, and B. D. Decker, "Privacypreserving
public transport ticketing system," in DBSec'15. Springer, 2015, pp. 135–150. [5] M. Mut-Puigserver, M. M. Payeras-Capell_a, J.-L. Ferrer-Gomila,
A. Vives-Guasch, and J. Castell_a-Roca, "A survey of electronic ticketing
applied to transport," Computers & Security, vol. 31, no. 8, pp. 925–939,
2012.

[6] A. Vives-Guasch, M. M. Payeras-Capell_a, M. Mut-Puigserver,
J. Castell_a-Roca-Roca, and J.-L. Ferrer-Gomilas, "Anonymous and
transferable electronic ticketing scheme," in DPM'13 and SETOP'13.
Springer, 2013, pp. 100–113.

[7] T. S. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu, "Privacy for
public transportation," in PET'06. ACM, 2006, pp. 1–19.

[8] G. Arfaoui, J.-F. Lalande, J. Traor_e, N. Desmoulins, P. Berthom_e, and
S. Gharout, "A practical set-membership proof for privacy-preserving
NFC mobile ticketing," in PoPETs'15. DE GRUYTER, 2015, pp. 25–
45.

[9] R. Song and L. Korba, "Pay-TV system with strong privacy and nonrepudiation
protection," IEEE Transactions on Consumer Electronics, vol. 49, no. 2, pp. 408–413, 2003.

[10] I. Gudymenko, "A privacy-preserving e-ticketing system for public
transportation supporting fine-granular billing and local validation," in
SIN'14. ACM, 2014, pp. 101–107.

[11] F. Kerschbaum, H. W. Lim, and I. Gudymenko, "Privacy-preserving
billing for e-ticketing systems in public transportation," in WPES'13.
ACM, 2013, pp. 143–154.

[12] A. Rupp, G. Hinterw◉alder, F. Baldimtsi, and C. Paar, "P4r: Privacypreserving pre-payments with refunds for transportation systems," in
FC'13. Springer, 2013, pp. 205–212.

[13] J. Camenisch, R. Chaabouni, and abhi shelat, "Efficient protocols for
set membership and range proofs," in ASIACRYPT'08. Springer, 2008,
pp. 234–252.

[14] IATA. (2012) Transferability of tickets. [Online]. Available: https:
//www.iata.org/policy/Documents/Transferability.pdf

[15] B. Patel and J. Crowcroft, "Ticket based service access for the mobile
user," in MobiCom'97. ACM, 1997, pp. 223–233.
[16] D. Chaum, "Blind signatures for untraceable payments," in Crypto'82.
Springer, 1982, pp. 199–203.
[17] D. Chaum and E. van Heyst, "Group signatures," in EUROCRYPT'91.
Springer, 1991, pp. 257–265.
[18] D. Chaum, "Security without identification: transaction systems to make
big brother obsolete," Communications of the ACM, vol. E28, no. 10,
pp. 1030–1044, 1985.
[19] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf, "Pseudonym
systems," in SAC'99. Springer, 1999, pp. 184–199.
[20] C.-I. Fan and C.-L. Lei, "Multi-recastable ticket schemes for electronic
voting," IEICE Transactions on Fundamentals of Electronics, Communications
and Computer Sciences, vol. E81-A, no. 5, pp. 940–949, 1998.
[21] D. Quercia and S. Hailes, "Motet: Mobile transactions using electronic
ticket," in SecureComm'05. IEEE, 2005, pp. 1–10.
[22] A. Rupp, F. Baldimtsi, G. Hinterw◎alder, and C. Paar, "Cryptographic
theory meets practice: Efficient and privacy-preserving payments for
public transport," ACM Transactions on Information and System Security,
vol. 17, no. 3, pp. 10:01–10:31, 2015.
[23] S. Brands, "Untraceable off-line cash in wallets with observers (extended
abstract)," in CRYPTO'93. Springer, 1993, pp. 302–318.
[24] D. Boneh, B. Lynn, and H. Shacham:, "Short signatures from the weil
pairing," Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004.
[25] M. Abe and T. Okamoto, "Provably secure partially blind signatures,"
in CRYPTO'00. Springer, 2000, pp. 271–286.