TSET: Token based Secure Electronic Transaction

Rajdeep Borgohain

Department of Computer Science and Engineering,

Dibrugarh University Institute of Engineering and Technology,

Dibrugarh, India

Moirangthem Tiken Singh

Department of Computer Science and Engineering, Dibrugarh University Institute of Engineering and Technology Dibrugarh, India

Chandrakant Sakharwade

DKOP Labs Pvt Ltd NOIDA 201301, India

Sugata Sanyal

School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India

ABSTRACT
Security and trust are the most important factors in online transaction, this paper introduces TSET, a Token based Secure Electronic Transaction, which is an improvement over the existing SET, Secure Electronic Transaction protocol. We take the concept of tokens in the TSET protocol to provide end to end security. It also provides trust evaluation mechanism so that trustworthiness of the merchants can be known by customers before being involved in the transaction. Moreover, we also propose a grading mechanism so that quality of service in the transactions improves.

General Terms
Network Security, Electronic Commerce, Mobile Computing.

Keywords
Secure Electronic Transaction, Token, Privacy, End to End Security,Trusted Third Party.

1. INTRODUCTION
Mobile payment is the transaction of fiscal values by means of mobile phones or other handheld devices. According to one of the Gartner's report [3] the total mobile users in the world will reach 7.4 billion by 2015. With such a large number of people using mobile devices, it would be increasingly used not only for communication but also as a means of monetary transactions [2].As mobile phones have become more and more powerful with multiple features, people would rather like to have their monetary transaction done with a mobile device rather than carrying currencies and notes in their pocket.

Though there are many existing mobile payment protocols, one of the most widely accepted mobile payment protocol is the Secure Electronic Transaction (SET) protocol [1]. Though SET has been accepted by many companies as the standard security protocol for online transactions, SET still has issues which need to be addressed [4]. SET does not provide a way for the customers to know the trustworthiness of the party they are dealing with [5]. This lack of trust is one of the prime reason people abstain from participating in online transactions and this has been a major hurdle for e-commerce. If there was a mechanism to know a priori the trustworthiness of the party the customers are dealing with, people would be more open to e-commerce. SET also does not guarantee the quality of products that will be available to the customers after the transaction, i.e. if the customer is not satisfied with the quality of the product after the transaction then SET does not provide

any mechanism by which the merchant becomes liable to provide a replacement or refund the amount of the product. Moreover, SET protocol does not provide any mechanism for end to end security [6]. The request for transaction can be compromised by any agency at any point in the transaction process [7] and lot more amount of money may be transacted than allowed by the customer without the knowledge of the customer.

In this paper, we propose a method, which enables people to know in advance the trustworthiness of the party customers are dealing with, provide a mechanism by which the customers would receive intended goods and provide end to end security of the transaction. To achieve the end to end security we introduce the concept of tokens which are generated by the customers' bank, based on which the transaction would be carried out. Any tampering in the token would indicate that the amount value in the transaction has been compromised and the transaction would not be allowed.

The rest of the paper is organized in the following way: Section 2 gives an overview of the SET protocol. In Section 3 we look at the disadvantages of the SET protocol. In Section 4 we introduce and discuss the TSET protocol. Section 5 gives an analysis of the TSET protocol, Section 6 gives a comparison of TSET with related worksand we finally conclude the paper in Section 7.

2. OVERVIEW OF SET PROTOCOL
The SET protocol is a security specification introduced by VISA and MasterCard for secure transaction over the internet. The main aim of the SET protocol is to ensure confidentiality of information. Secondly, it ensures the integrity of all the data that are transmitted during the transaction process. Finally, the SET protocol provides authentication that both the customer and the merchant are legitimate [8]. Both the customer and the merchant are provided with digital certificates that authenticate their legitimacy to make transaction over the network. The SET protocol basically involves the following entities: a Customer (Cardholder), Customer Bank (Issuer), Merchant, and Merchant Bank (Acquirer). Before participating in the transaction both the customer and the merchant must obtain a digital certificate from a Certifying Authority.

The steps involved in the SET protocol are:

1. The customer browses the website of the merchant and chooses the products.

2.The merchant returns a form containing the list of items along with total price and the order number. A copy of digital certificate is also sent for the authentication of the merchant.

3.The customer sends the dual signature order information and the payment information along with customer digital certificate. The digital certificate is to validate the customer's authenticity. The order information confirms that the customer will make the purchase, whereas the payment information is encrypted by the public key of the payment gateway which cannot be read by the merchant.

4.The merchant forwards the payment information to the merchant bank.

5.The merchant bank then forwards the information to the Customer Bank for authorization and payment.

6.The Customer Bank sends authorization to the merchant bank and merchant bank sends the authorization to the merchant.

7.The merchant completes the order and sends it to the customer.

8.The merchant captures the transaction from their bank.

9.The Customer Bank sends a notification to the Customer that the payment has been processed.

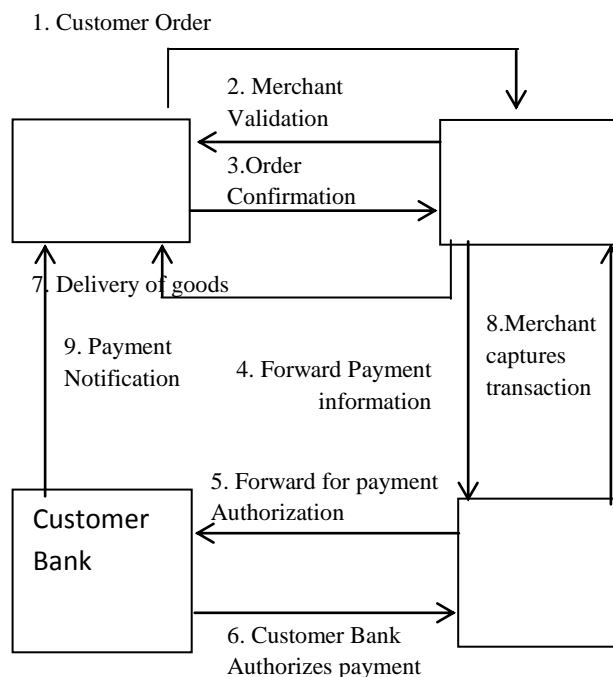The data model of the SET protocol is given in Figure 1.

Figure 1. The SET Protocol

The SET protocol was succeeded by 3D SET[10]. Visa and MasterCard introduced 3D SET in 1999, to facilitate flexibility and portability for customers. In 3D SET, the transaction logs are stored in the banks, as banks were deemed trusted entities by the customers [9].

3. LIMITATIONS OF SET PROTOCOL
The limitations of SET protocol are:

1.In the SET protocol there is no way in which the customer knows the trustworthiness of the merchant he is dealing with

[5]. The customers remain ignorant whether to trust the merchant with the deal or not. This is the main reason why many people remains skeptical about e-commerce, based on SET protocol.

2.The SET protocol does not provide any means by which the customer is assured that the goods that will be sent to him will be of the desired quality. If the products are not as per liking of the customer, the customer must be able to get a replacement or get a refund. This is not guaranteed by the SET protocol.

3.The SET protocol does not guarantee end to end security. During the transaction process the network may be hacked by any agencies at any point. If this happens the customer will end up paying much more than he intended to do without his knowledge. Moreover, in the traditional flow of transaction, there is fear of modification of balance by merchants [11, 12].

4.In SET protocol, the privacy of the customer is compromised [13]. Even in 3D SET the information regarding the payment and the order lies with the bank entities [9].The private information of the customers and the merchants can be accessed by the banks which could be misused by any third party who could get access to this information.

4. THE TSET PROTOCOL
The proposed protocol TSET, addresses the issues relating to trustworthiness of the merchants, ensuring customer satisfaction of the goods and end to end security. The TSET protocol involves the following entities, Customer, Merchant, Customer Bank, Merchant Bank and a Trusted Third Party (TTP). Usually, Secure Socket Layer (SSL)protocol is used by the TTP [14]. In this model, the Trusted Third Party works as a moderator between all the entities involved. The TTP stores the transaction log of the deals. In case of any disputes, the transaction log stored with the TTP is used to resolve the issues. It provides an undeniable proof of the transaction between the parties and as such issues like non repudiation cannot be raised. The TTP is also responsible for keeping track of the trust factor of the merchants. The trust factor of the merchant is stored with the TTP which the customers can access to analyze the trustworthiness of the merchant before getting involved with the transaction. Finally, the TTP also acts as an arbitrary body in case of any disputes.

The symbols used in the protocol are given in Table 1:

Table1. Symbols used in the protocol

Symbol	Meaning
C	Customer
M	Merchant
CB	Customer Bank
MB	Merchant Bank
$DCert_X$	Digital Certificate of entity X
AM	Amount
TS	Timestamp
TF_x	Trust Factor of entity X
OI	Order Information
TKN	Token
TKN_{req}	Token Request
PK_x	Public Key of entity X
SK_x	Secret Key of entity X
TID_x	Transaction ID by entity X

4.1 Calculation of the Trust Factor

The most important factor in the online transaction is the issue of trust. Even though people have the convenience of making online transactions from home and having products delivered at their doorsteps, people are still hesitant to indulge in online transaction activities. People are unsure of the other party which they deal with. If there is a mechanism which informs the customer, prior to the online transaction, how trustworthy the merchants are, people would be more open towards electronic commerce.

For calculating the trust factor of a merchant we propose a simple technique. The trust factor of a merchant involved in the transaction would remain with the TTP. At any point of time when the customer is about to involve in an online deal, he can log on into the website of the TTP and analyze the trust factor of the merchant. If the customer finds the trust factor of the merchant satisfactory he can proceed with the transaction and if he is not convinced with the trust factor of the merchant he can back away from the transaction. Trust factor can be calculated by the following formula,

$$TF_M = 100 - TV_M,$$

where TF_M = Trust Factor of Merchant.
TV_M = Trust Value of Merchant

The trust value of a merchant is decided by the total number of transaction the merchant is involved in and the total number of transactions where there had been a customer complaint and initial products were rejected. The trust value is calculated as,

$$TV_M = \frac{Number\ of\ times\ rejected\ by\ the\ customer}{Total\ number\ of\ times\ involved\ in\ transaction} \times 100$$

When a merchant gets refund or replacement request from the same customer for the same product more than once the trust value is calculated as $(TV_M)^2$, so that the customer does not have to go through the same ordeal again and again. The trust factor is divided into different grades given in Table 2.

Table 2. Grades distribution

TF_M	GRADE	TF_M	GRADE
100-90	A1	49-40	C2
89-80	A2	39-30	D1
79-70	B1	29-20	D2
69-60	B2	19-10	E1
59-50	C1	9-0	E2

Now, during the transaction the customer can view the trust factor of the merchant and decide himself whether he wants to participate in the transaction or not. For example, a certain merchant M_1 has a total of 1000 transactions and among them 25 of the transaction had replacement or refund of goods. So the trust value of the merchant M_1 becomes:

$$TV_{M1} = \frac{25}{1000} \times 100$$

$$= 2.5$$

So, the total trust factor TF_{M1} would be 97.5, which would assign a grade A1 to the merchant M_1.

On the other hand if a merchant M2 has 300 refunds out of a total 1000 transactions, the trust value of merchant M2 would become:

$$TV_{M2} = \frac{300}{1000} \times 100$$

$$= 30$$

So, the total trust factor TF_{M2} would be 70, which would assign a grade B1 to the merchant M_2.

Given a choice between the merchants, the customer would always go for merchant with the higher trust factor. This would give the customer a greater sense of trust to get involved in online transaction. Moreover, the merchants would always strive to provide highest quality of service to the customers so that their trust factor always remain as high as possible.

4.2 Format of the Token

For every transaction the Customer Bank generates a token which contains the information about total amount of the money to be paid, digital certificate of the customer, digital certificate of the merchant, Token ID, timestamp.

The first slot in the token contains information about the amount of money that has to be paid to the Merchant. The customer passes on this information to the Customer Bank in the order information OI. The Customer Bank will only release the amount of money mentioned in the token. The token also contains the digital certificate of the Customer and the digital certificate of the Merchant to verify that the token belongs to the particular Customer meant for the specific Merchant. There is also a Token ID which is unique to each transaction. The Token ID is a 256 bit code which is used once by the Customer Bank for every transaction. When the transaction for a particular Token ID is made, it is never generated again. A timestamp is also included in the token. The timestamp is included so that if any dispute arises, the arbitration body gets an authenticated proof of the date and time of the transaction. The structure of the Token is given in Figure 2:

AM	$DCert_C$	$DCert_M$	TKN_{ID}	TS

Figure 2. Structure of the Token.

The Token ID in the token is encrypted with AES symmetric key with the Rijndael algorithm [15]. The Customer Bank generates the symmetric key and decrypts it to check for any tampering in the Token when it is requested for the payment. The Customer Bank is obliged to payto the Merchant's bank only that amount of money that is embedded in the token. Moreover, the Customer's Bank keeps a duplicate copy of the Token every time the unique Token is generated. So, before releasing the transaction money, the Customer Bank compares the Token with the copy stored with it. If the Customer Bank finds any evidence of tampering in the Token, the transaction is stopped immediately. The Customer Bank then reports the TTP that the Token has been tampered with. The TTP then sends a message to the customer who requests the Customer Bank to generate a new Token and the whole process is carried out once again. So, the token ensures end to end security in the SET protocol, as any modification in the token will be immediately detected and the transaction process will be stopped.

The steps involved in the TSET protocol are:

1. The customer C browses the website of the merchant M and orders the goods.

Customer order

C ————————————————→ M

2.The merchant M sends his digital certificate DCertM along with the order information to the customer C to authenticate the merchant's validity.

$\{DCertM, OI\}\ PKC$

M ————————————————→ C

3.The customer logs into the TTP and checks the trust factor of the merchant. If the merchant is trustworthy of doing business, the customer proceeds to do the business otherwise abstains from it. If satisfied, the customer requests the Customer Bank CB for a token with the desired amount of money which the customer bank sends to the customer.

The transaction process of TSET model is shown in Figure 2

$\{TKN, OI, DCertC, TIDM\}\ PKTTP$

C————————————————→TTP

5. The merchant decrypts the message from the customer and after the authentication sends the TTP request for confirmation of the temporary payment. The TTP meanwhile decrypts the Token and checks for authenticity. If the TTP acknowledges the receipt of temporary payment in the form of token, the merchant dispatches the goods.

Temporary Payment Confirmation

M ————————————————→TTP

Dispatch Goods

M ————————————————→ C

Figure 3. The transaction process in the TSET protocol

$\{DCertM, TIDM, TKNREQ, OI\}\ PKCB$

C ————————————————→ CB

$\{TKN, DCertCB\}PKC$

CB————————————————→C

4.   The customer C sends the purchase confirmation to the merchant by sending his digital certificate and Order Information to the merchant.

$\{TIDM, OI, DCertC\}PKM$

C————————————————→M

At the same time, the customer C sends the order information and token to the TTP.

6. The customer after receiving the goods, if satisfied, sends a message to the TTP to release the token to the Merchant Bank MB. Otherwise, the customer asks the TTP to inform the merchant to replace the goods and hold the token for more time. In this case the trust factor of the merchant decreases.

Request to release token.

C ————————————————→M

7. The merchant bank MB upon receiving the token sends the token to the customer bank and request customer bank for payment.

$\{TKN, DCertMB\}\ PKCB$

M ─────────────────────────► CB
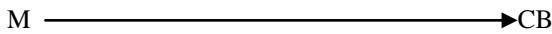
8. The customer bank on receiving the token decrypts the Token with its private key. The customer bank then decrypts the Token ID with its symmetric key and matches all the data in the Token against the data of the Token ID stored in its own database. It looks for any tampering in the token. If there is any tampering in the token, the CB reports it to the TTP that the token has

Payment

CB ─────────────────────────►MB

Payment Capture

MB─────────────────────────► M
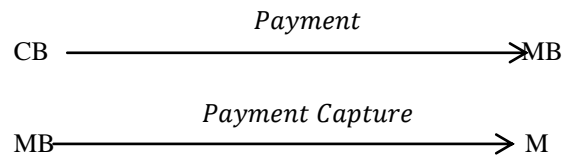
9. The merchant captures the payment from the Merchant Bank on completion of the transaction andnotifies the TTP about it.On the other hand, the Customer Bank CB after the final transaction informs the customer that the transaction has been completed.

Payment Information

CB ─────────────────────────► C
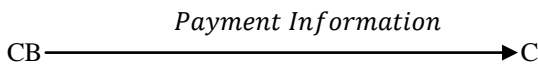
5. ANALYSIS OF THE SET PROTOCOL
This section discusses the various features of the TSET protocol.

5.1 Trust Mechanism
Based on the new TSET protocol the customers can now have a prior knowledge of the trustworthiness of the merchants. It is up to the customer if he wishes to continue his transactions with the merchant having a certain trust value. This mechanism also ensures that the merchants will only provide the authentic products as desired by the customer otherwise their trust factor falls which has an impact on their business.

5.2 Quality of Service
The new protocol entitles the customer to return the goods if he is not satisfied with it. The TTP acts as the governing body and ensures that the merchant provides a replacement or refund of the product within a stipulated period of time. Failing to resolve the discrepancy leads to decrease of trust factor of the merchant. This will not be desired by the merchant. So this protocol ensures that the merchant provides only products of the highest quality as desired by the customers.

5.3 End to End Security
The new SET protocol ensures end to end security. At no point in time of the transaction can the Token, where the amount of transaction is embedded can be compromised by any agency. If the Token is altered and the amount embedded in the Token is tampered, the Customer Bank detects it by matching it with copy of token in its database. Evidence of any tampering will immediately result in halting of the transaction process and a new token will be generated. So, this ensures that the merchant will only get the desired amount of money as provided by the customer.

5.4 Disputes
As every transaction has to pass through the TTP, it ensures a fair trading between all the parties. If there arises any dispute regarding the transactions, the TTP can provide the transaction log between the two parties. This record cannotbe denied by either party and thus there can be settlement based on this record.

5.5 Privacy
The protocol also partially fulfills the security requirements as mentioned in [9]. The customer information is not known to the merchant or the merchant bank at any point of the transaction. Moreover, the order information is known only to the customer and merchant.

6. COMPARISON WITH RELATED WORKS
Many researchers have proposed improvement of the existing Secure Electronic Transaction Protocol. Here we present a comparison of the existing improved Secure Electronic Transaction Protocol with the TSET protocol:

Table 3. Comparison with related works

Related Works	Features
Ren *etal.*	The paper introduces data destructionmechanism, the concept of pre-payment mechanism and aserver to store records to improve the SET protocol.
Boping and Shiyu	Introduces concept of electron transaction authentication center for improvement of security.
Yong and Jondi	Introduces a payment system based on simplified model of the Secure Electronic Transaction Protocol and Trusted Third Party.
Tiwari *et al.*	Introduces multifactor authentication for online transactions. Provides application layer security solution for end to end data authentication and data confidentiality.
TSET	TSET introduces end to end security based on tokens encrypted by AES symmetric key. It also introduces trust evaluation for authenticated transactions and quality of service.

In [5] Ren *et al.* proposed an improvement over the Secure Electronic Transaction by introducing data destruction mechanism. The paper also introduced an evaluation mechanism by which the customers were able to make a prepayment based on transaction history of the merchants stored in the server.In [1], Boping and Shiyu proposed the concept of authentication center which would improve the security of the Secure Electronic Transaction. In [14], Yong and Jondi proposed a simplified version of Secure Electronic Transaction combined with trusted third party. In [6, 11], an improvement of end to end security of the SET protocol was proposed by Tiwari *etal.* based on multifactor authentication. The TSET protocol proposed in this paper has added some significant features to the Secure Electronic Transaction

Protocol. It is an improvement over the Secure Electronic Transaction Protocol as it has added features of evaluating trust of merchants, ensuring quality of service, providing end to end security, resolving disputes and ensuring privacy of the customers.

7. CONCLUSION

In this paper the Token based Secure Electronic Transaction for mobile payments has been discussed. We primarily focused on the trust factor and end to end security of the protocol and quality of service. Depending on the different trust values assigned to the merchants, the customers can now be sure of the trustworthiness of the merchant before indulging in the transaction process. The end to end security mechanism ensures that a faulty transaction never takes place and only the actual amount of money is released to the merchant. Because of the grading mechanism, the merchant will always try to provide good quality products to the customers so that their trust factor remains high. We believe that by increasing the trust of customers, improving the security of TSET protocol and by providing better quality of service, more and more people will be open towards electronic commerce.

8. REFERENCES

[1] Boping, Z and Shiyu, S.: "An Improved SET Protocol", Proceedings of the 2009 International Symposium on Information Processing (ISIP'09),Huangshan, P. R. China, 2009, pp. 267-272.

[2] Ding, M.S and Unnithan, C.R., 2002, "Mobile PaymentsmPayments) –An Exploratory Study of Emerging Issues and Future Trends", Information Technology and Organizations Deakin University.[online] Available at http://www.idea-group.com, pp. 99-101.(Accessed 15 February, 2012)

[3] Pettey, C. "Gartner Says Worldwide Mobile connections Will Reach 5.6 Billion in 2011 as Mobile Data Services Revenue Totals $314.7 Billion", 2011, [online] Available at http://www.gartner.com/it/page.jsp (Accessed 21 February, 2012).

[4] Boudriga, N., "Security of Mobile Communications", 2009, CRC Press, USA. ISBN 0849379415.

[5] Ren, X.Y., Wei, L.L,Zhang, J.F andMa, X., "The Improvement of SET Protocol based on Security Mobile Payment", Journal of Convergence Information Technology, Volume 6, Number 7, 2011, pp. 22-28.

[6] Tiwari, A., Sanyal,S., Abraham,A and Sanyal,S., "A Multifactor Security Protocol For Wireless Payment-Secure Web Authentication using Mobile Devices", IADIS International Conference, Applied Computing 2007, Salamanca, Spain, 2007, pp. 160-167.

[7] Vasudevan, R.A. and Sanyal, S., "A Novel Multipath Approach to Security in Mobile and Ad Hoc Networks (MANETs)", Proceedings of International Conference on Computers and Devices for Communication CODEC'04), Kolkata, India, 2004, pp. CAN_0412_CO_F_1 to CAN_0412_CO_F_4.

[8] Li, Y andWang, Y., "Secure Electronic Transaction (SET protocol)",2001, [online] Available at http://www.people.dsv.su.se/~matei/courses/IK2001_SJE /li-wang_SET.pdf (Accessed 15 February, 2012).

[9] Hwang, J.J., Yeh, T.C and Li, J.B., "Securing on-line credit card payments without disclosing privacy information". Computer Standards and Interfaces, Volume 25, Number 2, 2003,pp. 119-129.

[10] VISAEU,3D SET, [online] at http://www.visaeu.com/virt

ual_visa/merchants/3dset.html. (Accessed 25 January, 2011)

[11] Sanyal, S., Tiwari, A andSanyal, S., "A Multifactor Secure Authentication System for Wireless Payment" , Emergent Web Intelligence: Advanced Information Retrieval Book Series: Advanced Information and Knowledge Processing, First Edition, 2010, Chapter 13, pp. 341-369, XVI, Springer Verlag London Limited, 2010.

[12] Goyal,V.,Kumar,V., Singh, M., Abraham, A andSanyal, S. "CompChall: Addressing Password Guessing Attacks", Information Assurance and Security Track (IAS'05),2005, IEEE International Conference on Information Technology: Coding and Computing (ITCC'05), USA. April 2005, pp. 739-744, IEEE Computer Society.

[13] Fun,T.S., Beng,L.Y.,Roslan, R and Habeeb, H.S., "Privacy in New Mobile Payment Protocol", In Proceedings of World Academy of Science, Engineering and Technology, Vol.30,2008, pp. 443-447.

[14] Yong, X., Jindi, L., "Electronic Payment System De-sign Based on SET and TTP", 2010 International Conference on E-Business and E-Government, Guangzhou, 7-9 May 2010, pp. 275-278.

[15] Daemen, J andRijmen, V., "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2.