IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-3, Issue-8 E-ISSN: 2347-2693

A Survey on Various Online Transaction, E-Commerce Security and Applications

Varsha Jotwani[1*] and Amit Dutta[2]

[1*] *Department of Computer Science, Aisect University, India*
[2] *Department of Computer Science , Barkatullah University, India*

www.ijcseonline.org

Received: Aug /02/2015 Revised: Aug/12/2015 Accepted: Aug/27/2015 Published: Aug/30/2015

Abstract-While the usage of ecommerce application, information and communication technology enhances in private and professional existence, personal data is extensively stored. While service providers require relying on recognizing their consumers, aware characteristics administration and privacy increases into a new assessment for the service user, particularly in the electronic service circumstance. At this time, recent technology infrastructures can support in on condition that security to both sides by assuring identification and privacy at the same time.

***Keywords*—**Trusted Platform Module,Trusted Computing Group,Security,Security

I. INTRODUCTION

As today's software is becoming more and more mobile and inherently networked, and its tasks get progressively more significant, methods should be in position to begin trust relationships between computing platforms. For instance, in online banking the bank wants be assured that a financial transaction is generated by a legitimate client of the bank and not by malware that has infected the client's computer. E-commerce application and individuals are assigning progressively greater amounts of security-sensitive data to computers, both their individual and those of third parties. To be admirable of this expectation, these computers must ensure that the data is handled with care (e.g., as the user expects), and protected from external threats. A progressively more IT-based and virtual mode of human contact in the business and private world as they enable services such as payment, access and multimedia-based communication. They are becoming important enablers in the identification of individuals. Further, internet-based services are increasingly provided through mobile devices. Hence, the security and privacy issues that already exist in the World Wide Web gain importance for the mobile world too.

In this context, the two parties of a service i.e. the provider on the one side and the client on the other increasingly distinguish service security as a crucial selling proposition. At the same time, service quality is becoming a non-differentiating essential constraint. From a service provider point of view, the security of a service is reliant upon the identification of the respective individual in the specific service encounter. From a customer perspective, security roots in the minimum possible transmission of the specifically needed personal data and the highest possible level of privacy for the data that is transferred.

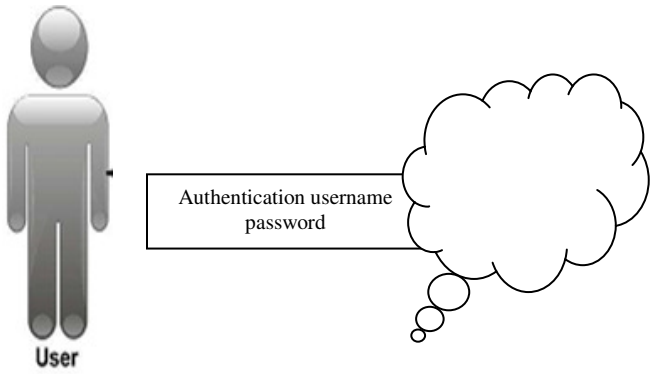

Figure.1: Secure Service Provision

Unfortunately, today's computer platforms provide little assurance on either front. Most platforms still run code designed primarily for features, not security. Trusted computing technology is a relatively new enabling technology to improve the trustworthiness of computing platforms. With minor changes to the boot process and the addition of a new hardware security component, called TPM (Trusted Platform Module), trusted computing platforms offer the possibility to verifiably report their integrity to external parties (i.e., remote attestation) and to bind information to a specific platform (i.e., sealed storage). The Trusted Computing Group (TCG), an industry usual organization, has particular a TCB for trusted computing in the structure of three so-called roots of trust: the root of trust for storage (RTS), the root of trust for reporting (RTR), and the root of trust for measurement (RTM). Especially, the TCG has particular a Trusted Platform Module (TPM) [1] that can act as together roots of trust for storage and size.

The main initiative for a new generation of computing platforms was taken by the Trusted Computing Platform

© 2015, IJCSE All Rights Reserved

Alliance (TCPA), an association of a large amount major IT companies, and its successor the Trusted Computing Group (TCG). This proposal chooses for a dissimilar move toward those values the honesty of the PC platform. A TCG allowed platform consistently computes the software components that get loaded during startup by calculating their cryptographic hash and records these measurements in a hardware security module, the Trusted Platform Module (TPM). This approach is called authenticated boot, determined boot or trusted boot. Calculated boot does not enforce constraints on the operating system that the proposal can boot, as the TPM merely operates as a logging device that does not actively intervene in the bootstrap process. This means that the platform can start into an arbitrary but provable condition. After establish, the platform condition can be reported to an inaccessible entity with an confirmation protocol or it can be used to securely bind secrets to a specific platform configuration in a process commonly referred to as sealed storage space. The earlier make possible service providers to confine access to a network service based on the determined platform arrangement and distinctiveness.

The remote attestation provided by TCG platforms has a number of problems which maximum value convenient exploitation. Initially, in its original form the TCG attestation process masquerade some privacy apprehensions, which are partly concentrate on the Direct Anonymous Attestation (DAA) protocol [2, 3] of the TPM specification. Secondly, binary measurement of the platform configuration has scalability issues because managing the multitude of possible configurations can be difficult, and permits for unfairness of definite arrangements. Lastly, attestation of individual applications [4] necessitates a secure operating system.

II. SECURITY CONSIDERATIONS AND ITS CONCEPT

In the services industry – and particularly in services which are based on electronic devices – a new paradigm seems to be emerging: The conscious management of identity in a secure service context. Quality of Service (QoS) has already become an indispensable attribute as a foundation to this understanding. Hence, QoS is already defined in the deployment of any service architecture. Treating Security of Service (SoS) [4] as a similarly crucial attribute of a service calls for an exploration and definition of the term. It is obvious that security needs a kind of trust secure. Such a security attach allows the user:

- To define a secure domain, which also is context-dependent (home/family, friends, work, travel).
- To deal with the user's individual background so that the management of the user's device base is both secure and easy.
- To define which of his devices can be publicly or restrictedly accessed and how interactions occur.

A secure client in combination with a trusted component in a mobile device can serve as a security anchor in the overall SoS concept [5] and system architecture. The Security of Service (SoS) concept can be expected to expand alongside three phases. These phases are not only significant to await the distinctiveness of upcoming security constraints, but can also assist to pin-point the definition of the concept alongside its anticipated path of development. Therefore, essential the SoS-concept [5] could be accomplished in 3 steps. These match the respectively needed capability tiers:

Security requirements in a static environment: This will consider fixed and concrete client and server components, actors and scenarios. The definition of SoS will result in fixed security requirements for the given circumstances. At this stage, SoS behavior can be increased and modified in the client and server component.

Security rules in a dynamic environment: This will consider the heterogeneity of scenarios. The definition of SoS will result in security rules. The equipment, context-aware, will know rules of behaviour under unusual circumstances. The SoS will be transformed in a condition-definite manner according to the rules defined during the pre-expansion. For this reason, the SoS is dynamic and co-develops with the isotropic and steadily changing context into which it is embedded. This move toward is comparable to the technique in which Europay, Mastercard, and Visa (EMV4) consider security in different and continuously changing scenarios.

Security policies in an adaptive environment: This will consider unidentified tools, actors, and heterogeneity of gap. The explanation of SoS will consequence in security policies. The client and the server will know the policies. Both will consider whether a given service is to be continued or blocked for a dedicated actor in definite circumstances. In an adaptive environment, QoS and SoS take a "flexible and safe", "pervasive and protected", "resilient and sheltered", "recoverable and safe" character, depending on the condition. The user and the server components will deploy an adaptive SoS and QoS ad hoc by negotiating the SoS according to the agreed security policies.

Currently, a high level of security of environment can especially be achieved through mobile devices such as Smart Cards. Other approaches can be based on virtualization [7], secure bootstrapping [6], ARM Trust Zone [8], or a combination thereof. The isolation of the secure environment (or the Smart Card as secure Component in a wider service context) is a key advantage. Further, the often small size of the Smart Card-related systems can reduce the complexity of probable attacks. On the other hand, this small amount may also consequence in limited computing power and memory capacity. Still though, Smart Cards can serve as an excellent starting point for all applications in which a higher level of security is necessary and the potential limitations of capacity do not hinder the implementation. This can be particularly promising if Smart Cards are combined with other secure environments in a mobile device [7], [8].

© 2015, IJCSE All Rights Reserved

III. Capabilities of Smart Cards and Token Technology

The main usage of Smart Cards is the storage of highly confidential information, for example cryptographic keys, and the implementation of safety measures critical processes, such as an authentication to prove the identity of a person or device. Classical Smart Card use cases are [9], [10]:

- Authorization in announcement networks, such as mobile phone networks or the Internet,
- Execution of security-critical processes with banking and payment applications, e.g. credit and debit operations on an electronic purse,
- Storage of sensitive personal information, e.g. on health and identity cards,
- Physical and logical access control.

Major Smart Card milestones in the past were the introduction of the SIM (Subscriber Identity Module) as the security device in mobile networks and the invention of Java on Smart Cards, i.e. the JavaCard™ Standard. With JavaCard™ the flexibility of Smart Cards amplified, because it was the initial time achievable to develop Smart Card applications in an interoperable format. The so-called JavaCard™ Applets can be executed in an almost interoperable manner on different JavaCards™ from different Smart Card vendors. With the ever-increasing computing capability of µProcessor Smart Cards new opportunities appear. Newer Smart Cards, connected to a host over the USB interface, present a full TCP/IP stack in the operating system. These Internet-Smart Cards no longer depend on a PC to be able to communicate because they can act independently as a network node in a global network like the Internet. So, they possibly will provide as a good security mechanism for personal data in combination with information exchange in a cross-domain network. A person can determine, which information about her/him/is published by help of the communication gateway Internet-Smart Card that supports standard Web technologies like HTML (hypertext markup language) pages and HTTP (hypertext transfer protocol). Therefore, the Internet-Smart Card [11] hosts a Smart Card Web Server (SCWS) which acts as graphical user interface for the individual token. The Internet-Smart Card expertise and SCWS also appear in the future USIMs in mobile networks. On the client side, a web-like look and think simplifies information exchange with a Smart Card. such as, clients browse a phone book or FAQ list based on HTML pages stored directly on the Smart Card Web Server (SCWS) hosted on the (U) SIM. On the provider side, an HTTP-based keep informed mechanism simplifies the exchange of content with previously issued (U) SIMs. In conjunction with the Internet technology on Smart Cards, the assortment of dissimilar data types accumulated on the Smart Card and delivered by the SCWS is considerably increasing.

IV. Trusted Computing and its Platform Module

Trusted computing initiatives intend to solve some of today's safety measures crisis of the fundamental computing platforms from side to side hardware and software transforms. The most important initiative for a new generation of computing platforms is the TCG, a grouping of a large amount major IT companies. Trusted computing is a rather new technology driven by the Trusted Computing Group (TCG) [12]. Its goal is secure personal computing. Unlike the usual procedure of finding a fixing bugs which allow an attacker access to a system trusted computing uses cryptography to measure a systems condition. The system's condition depends on the software components which are executed as well as on the sequence of implementation. Any situation transform designates revolutionize in software system. An alteration in software system can be generated by a regular software update as well as by a piece of injected malicious code. The foundation of the scheme circumstances transform has not to be known.

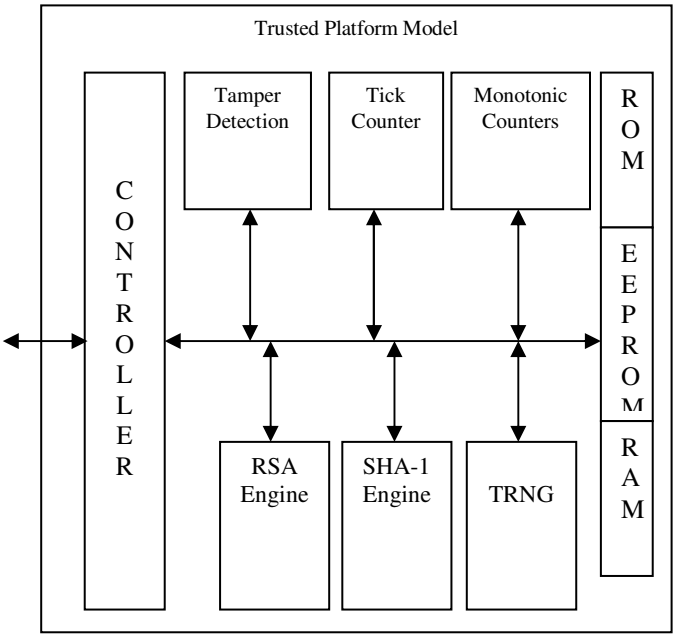

Figure.2: Simplified architecture of TPM

The TPM is a smart card like hardware module that was originally envisioned to be platform investigative. On the other hand, actually the requirement is primarily designed for the PC platform and therefore the TCG later on made a specification for a hardware module more tailored for advanced mobile devices such as smart phones and tablets, called MTM. The MTM condition appends some mobile specific functionality and declares (mandatory) TPM features optional in order to minimize the footprint of the module [13]. The TPM has to be strongly jumped to the rest

© 2015, IJCSE All Rights Reserved

of the platform. Figure 2.1 gives a schematic overview of the internal architecture of a TPM version 1.2. The trusted component exchanges a few words with the central microprocessor of the platform over an I/O bus. The Low Pin Count (LPC) bus is the regulated interface for PCs to communicate with a TPM.

V. ARCHITECTURE OF A TRUSTED COMPUTING PLATFORM

The basis of every system is some kind of platform. In a trusted computing platform the platform includes a TPM as well as a Root of Trust for Measurement (RTM). Ahead of the platform there is the operating system which manages resources, provides hardware drivers and almost immediately. The hardware driver of the TPM is called TPM device driver (TDD) and operates in benefited method. It is making available by the dealer of the TPM. In addition the PM the TCG Software Stack (TSS) is the second important part of a trusted computing platform. The TSS runs as unprivileged system process inside the operating system. It is created of three logical parts: the TCG device driver libraries (TDDL), the TCG core service (TCS), and the user library TCG service provider (TSP) [14]. The structural design characterized by the TCG is a layer-based design. In theory, each layer can be exchanged without touching adjacent layers. See Figure 3 for an overview.

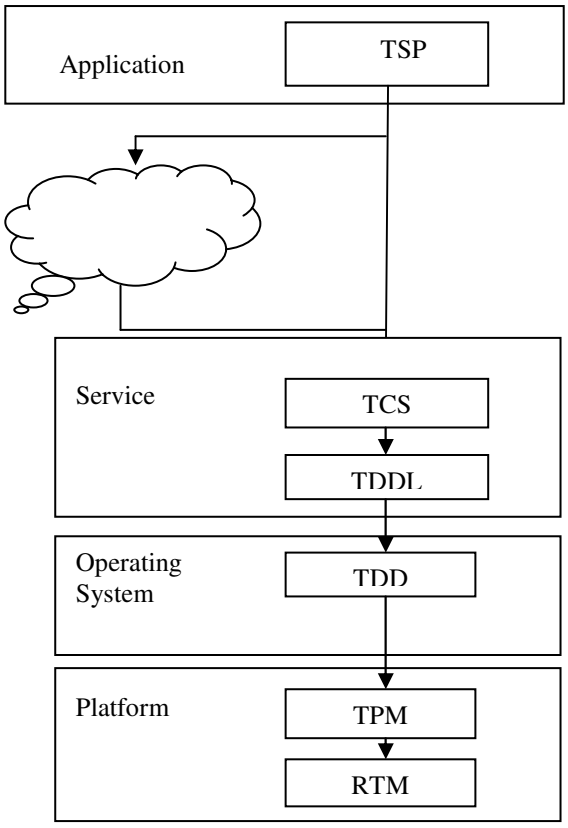

Figure.3: Architectural overview of a trusted computing platform [14]

In order to create a trusted computing platform, a devoted hardware safety measures module called Trusted Platform Module (TPM) is included in the specification of the TCG. The TPM is very similar to a Smart Card (SC). It provides cryptographic services, storage, key management as well as other protected capabilities accessible via a well described crossing point. In addition, alter conflict alongside software attacks is put into practiced. The main distinction to Smart Cards is that the TPM is physically bound to its host platform. Consequently, the TPM can identify the uniqueness of its platform with its Endorsement Key (EK). That permits procedures such as detection or authentication. Disadvantages such as privacy problems happen as well. Furthermore, TPMs should be devices which do not have great cost impact on host systems. On the one hand, this helps scattering trust and trusted computing (TC) to every digital machine. Alternatively, a resource presented by the TPM such as speed and memory remain small and therefore only a small set of services is feasible.

VI. LITERATURE SURVEY

This paper describes important security issues in E-commerce. Through the analysis, the customers and the organization to join those in a single phenomenon with respect to E-commerce security. By such analysis of information, it generates a "holistic" view. It will reduce the gap between organization and the customer's objectives and their perceptions. By the holistic view of analysis, information about customer and the open Internet organization implement such solution which aligned the customer needs more effectively [15]. Secure Electronic Transaction is communication protocol standard and an encryption and security specification protocol for securing credit card transactions in open network called Internet during E-commerce transactions. SET is not a payment system but it is security standard and a combination of security protocols and formats. This enables the users to online transaction through their credit card in unlock network. SET is a protected announcement open standard which provides privacy and protection to ensure the authenticity of electronic transaction. Privacy is more important for user security. Without confidentiality, any user can not at all be authenticated as consumer and without verification, neither the commercial nor the user cannot be sure that a valid transaction is being made. SET is an important part of E-commerce [16].

The advantages and requirements of the proposed token are also discussed in the paper.

- Network Security Issues in e-Commerce.[17] by Raghav Gautam, Sukhwinder Singh in which their advantages in this paper is "Give Dimensions of e-commerce security for not dangerous and secure online shopping through shopping web sites" and Issues- "Enlightening the user on security issues is unmoving in the formative year's period.

© 2015, IJCSE All Rights Reserved

- Designing A Logical Security Framework." For E-Commerce System Based On SOA.[18] by Ashish Kr. Luhach, Dr. Sanjay K. Dwivedi, Dr. C. K. Jha and their advantages of "SOA is also provided with no difficulty for message corrupting and unauthorized access. It is also being moderate to use, elastic, reusable, and scalable." Issues- "Primarily issue to determine the security of SOA based E-commerce."
- Transaction Security for Internet E-commerce Application.[19] by Khandare Nikhil B their advantages "Privacy of payment card information because of revelation of this information to malicious challenger could allow them to execute fraudulent transactions at the customer's cost."Issues - Privacy and Security are the two main issues that have an effect on users trust in electronic transaction."
- E-commerce Security through A-Symmetric Algorithm [20] by Ankur Chaudhary, Khaleel Ahmad, M.A. Rizvi their advantages are "It produces much iteration and takes in excess of time to development the data in the verification but they used RSA algorithm which is the largest part safe and less time unbearable."Issues- "Security issues should have some secure conditions that should give the sufficient defense to the transaction in order for each and every thing in E-commerce transaction."
- A Compliant Assurance Model for Assessing the Trustworthiness of Cloud-based E-Commerce Sysgtems.[21] by Thembekile O. Mayayise, Isaac O. Osunmakinde and their advantages are "Major advantage is to have an intellectual cloud-based declaration rating and can be used by online clients, dealers, cloud service providers and also law enforcers." Issues-" Challenges are deal with to facilitate give confidence online user trust based on declaration model for e-commerce."
- Contextualization of Geographical Scrapped data to support Human judgment and classification[22] by Luca Mazzola, Aris Tsois, Tatyana Dimitrova, and Elena Camossi and their advantages is "The technique can help in ever-increasing the data quality, and as a result support in the analysis procedure ." Issues – "Here issue is to address is as soon as a text string recognizing a location the location of a affecting object, cannot be equivalent with self assurance using string relationship to any particular position in the reference list."

VII. CONCLUSION

The market analysis of various e-commerce application we did gave us an suggestion on what a protection component is, what it does, how it does what it does, how high-speed computing and safe it does what is does, and on the collision of expenditure. The information draw together showed an opening e-commerce application advertises. Business modules are also low-cost or high-cost and less make safe or more protected correspondingly.

VIII. REFERENCES

[1] Trusted Computing Group: TCG TPM specification version 1.2. (TCG Specification).

[2] Brickell, E. F., Camenisch, J., and Chen, L. Direct Anonymous Attestation. In 11th ACM Conference on Computer and Communications Security (CCS 2004) (**2004**), V. Atluri, B. Pfitzmann, and P. D. McDaniel, Eds., ACM, pp. 132–145.

[3] Camenisch, J. Better Privacy for Trusted Computing Platforms: (Extended Abstract). In 9th European Symposium on Research In Computer Security (ESORICS 2004) (**2004**), P. Samarati, P. Y. A. Ryan, D. Gollmann, and R. Molva, Eds., vol. 3193 of Lecture Notes in Computer Science, Springer, pp. 73–88.

[4] Sailer, R., Zhang, X., Jaeger, T., and van Doorn, L. Design and Implementation of a TCG-based Integrity Measurement Architecture. In 13th USENIX Security Symposium (**2004**), USENIX, pp. 223–238.

[5] A. D. Keromytis, V. Misra, and D. Rubenstein. SOS: Secure overlay services. In Proceedings of ACM SIGCOMM, **2002**.

[6] TCG (2008) TPM Spezifikationen der Trusted Computing Group [Specifications of the Trusted Computing Group], https://www.trustedcomputinggroup.org/specs/TPM,.

[7] European Multilaterally Secure Computing Base (EMSCB) (**2008**) Turaja Technology, http://www.emscb.de/content/pages/About-Turaya-de.htm,.

[8] ARM (2008) ARM processor architecture, security extension ARM Trust Zone technology, http://www.arm.com/products/esd/trustzone_home.html, .

[9] Rankl, W.; Effing, W. (**2002**) Handbuch der Chipkarten, 4th edition, Munich, Carl Hanser Verlag.

[10] Swoboda, J., Spitz, S., Pramateftakis, M. (2008) Kryptographie und IT Sicherheit, Wiesbaden, Vieweg-Teubner, ISBN 978-3-8348-0248-4.

[11] InspireD (**2005**) D6 Communication Architecture Definition (Draft), forthcoming on http://www.inspiredproject.com,.

[12] Trusted Computing Group. http://www.trustedcomputinggroup.org/ (05 April **2010**).

[13] Ekberg, J.-E., and Kylänpää, M. Mobile Trusted Module (MTM) – an introduction, Nov. **2007**. http://research.nokia.com/files/NRCTR2007015.pdf.

[14] D. Challener, K. Yoder, F. Catherman, D. Saord, and L. V. Coorn. A Practical Guide to Trusted Computing. Pearson plc IBM press, **2008**. ISBN-13: 978-0-13-239842-8.

[15] http://www.ecommerce-digest.com/7_8.html. (Accessed 23 Sept **2013**).

© 2015, IJCSE All Rights Reserved

[16] Christoph Kern, Anita Kesavan, and NeilDaswani, Foundations of Security: What Every Programmer Needs to Know.

[17] Raghav Gautam, Sukhwinder Singh, "Network Security Issues in e-Commerce" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March **2014**.

[18] Ashish Kr. Luhach, Dr. Sanjay K. Dwivedi, Dr. C. K. Jha. "Designing A Logical Security Framework For E-Commerce System Based On SOA" International Journal on Soft Computing (IJSC) Vol. 5, No. 2, May **2014**.

[19] Khandare Nikhil B., "Transaction Security for Internet E-commerce Application" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February **2015**.

[20] Ankur Chaudhary, Khaleel Ahmad, M.A. Rizvi, "E-commerce Security Through Asymmetric Key Algorithm" Fourth International Conference on Communication Systems and Network Technologies, **2014**.

[21] Thembekile O. Mayayise, Isaac O. Osunmakinde, "A Compliant Assurance Model for Assessing the Trustworthiness of Cloud-based E-Commerce Systems" **2014**.

[22] Luca Mazzola, Aris Tsois, Tatyana Dimitrova, and Elena Camossi, "Contextualisation of Geographical Scraped Data to Support Human Judgment and Classification" European Intelligence and Security Informatics Conference, **2013**.

© 2015, IJCSE All Rights Reserved