VAN based theoretical EDI framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models

[1]Onurhan YILMAZ,[2]Zeynep Büşra KİRENCİGİL,[3]Arif SARI
Department of Management Information Systems
Girne American University, Turkey
onurhanyilmaz87@gmail.com zeynepkirencigil@gmail.com arifsari@gau.edu.tr

Abstract— Cryptography is a very powerful tool for Business-to-Business (B2B) data transaction security. The overall volume of B2B transactions is much higher than the volume of Business-to-Consumer (B2C) transactions and data security is very important due to volume and value of data in B2B transactions. Organizations that use cryptographic data security models to enhance security for business transactions deal with variety of unauthorized data manipulation problems. Researchers have proposed variety of cryptographic solutions to enhance security for B2B transactions. Companies should include cryptographic security models into organizational security policy to enhance security for transactions. This research paper highlights the detailed comparison of pros and cons of available cryptographic methods used to enhance security for B2B transactions and proposing theoretical Value Added Network (VAN) based Electronic Data Interchange (EDI) framework in order to enhance security between B2B transactions.

Index Terms— Minimum 7 keywords are mandatory, Keywords should closely reflect the topic and should optimally characterize the paper. Use about four key words or phrases in alphabetical order, separated by commas.

1 Introduction

The widespread of the Internet technology and virtualization of business companies lead a significant increase in B2B transaction volume. Company's transactions attract attackers to launch variety of attacks to these data during transmissions since the majority of the business transactions contain private data such as credit card details, personal information, bank account details etc. Companies have proposed and used variety of data encryption and cryptographic techniques to enhance data security during transmission. There are many possible solutions available for data security and companies have to choose the best option among the alternatives to prevent loss of profit, data and reputation. Attackers generated %9 of attacks in 2013 aimed specifically at organizations or brands. The companies suffered a cyber-attack at least once a year through variety of attack mechanisms, viruses, worms, network intrusion attacks, DoS-DDoS attacks, corporate espionage, theft of larger hardware or phishing attacks shown in Figure 1 below.

.

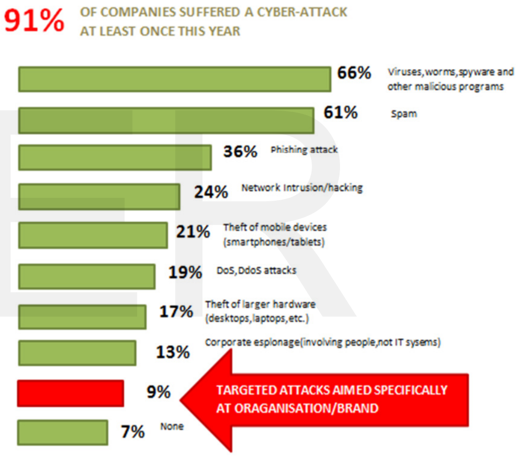


Figure 1. Cyber attacks generated against B2B transactions in 2013

This research examines the proposed cryptographic applications used in B2B transactions to enhance electronic data interchange (EDI) between B2B e-commerce type companies. In addition to this, the proposed theoretical Value Added Network (VAN) based Electronic Data Interchange (EDI) framework in order to enhance security between B2B transactions. The section 2 of this research paper covers the volume of B2B transactions, and discusses details about existing solutions provided in the market such as CryptoFlow, Trend Micro and PKI. The section 3 exposes the differences between cryptographic data security solutions used for B2B transactions with comarative survey. The section 4 explains the proposed theoratical Value Added Network (VAN) based Eelectronic Data Interchange (EDI) model to enhance organizational data security for B2B transcations and concluding the research.

2 Business-to-Business (B2B) Transactions

B2B transactions are the largest form of e-commerce involving business of trillions of dollars. This model defines commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer. The development and usage of B2B e-Commerce enabling technology has caused profound changes in the e-Business environment. The B2B e-Marketplace can significantly improve the way companies deal with their customers and suppliers. The overall volume of B2B transactions is much higher than the volume of Business-to-Consumer (B2C) transactions. *"For example, an automobile manufacturer makes several B2B transactions such as buying tires, glass for windscreens, and rubber hoses for its vehicles"* [1].

B2B commerce type is more beneficial than all other business types among different e-commerce types for the companies. Because it makes easier purchasing, payment, and inventory processes while providing special product assortment, pricing and business flows.

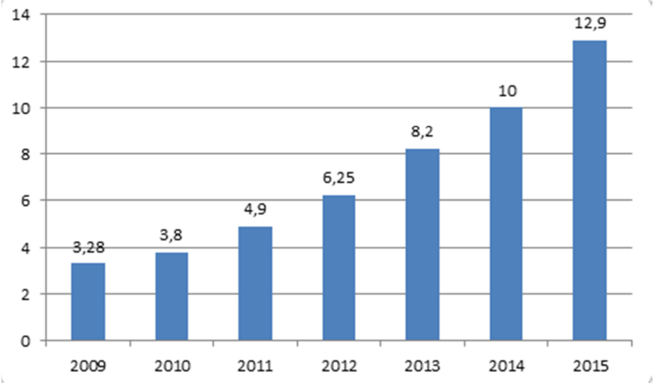
In the following there are two types business model. These are Dell Business Model and Cisco Business Model.

The Dell Business Model
One of the business models for B2B model is the Dell business model. In this model orders placed with dell by telephone or Internet. Actually productivity needed for manufacturing required inventory is improved. Under the just-in-time philosophy, under the just-in-time philosophy, Dell only orders the parts for a computer when it has a firm (and in the case of non-corporate orders, prepaid) order. Products are produced and shipped short time. On the other hand, product is not produce by Dell; it is shipped directly to customer from producer. These are all possible solutions for decreasing cost of production and sales [2].

The Cisco Business Model
Other B2B model is Cisco business model. It is takes the orders approximately 90 percent on the Internet. *"The orders are routed to contract electronics manufacturers who build the products to Cisco's specifications."* All of the orders not on the web, but 70 to 80 percent customer service with online [2].

B2B e-commerce is growing every day. In the following tables show the change of B2B ecommerce volume in China and USA. The impact of this growth is also stated by the researchers in the literature by stating the diversification of technology in business by deploying different data centers to compute huge amount of data from B2B transactions [3].

Transaction volume of B2B e-commerce in China from 2009 to 2015 (in trillion yuan)



This Figure 2 shows above the change of volume in China between 2009 and 2015. Everyear volume is increase. In 2009 volume is 3.28 trillion yuan, in 2015 volume is 12.9 trillion. It is approximate %400 increasing between these years[4].

B2B e-commerce volume in the United States from 2006 to 2012 (in billion U.S. dollars)

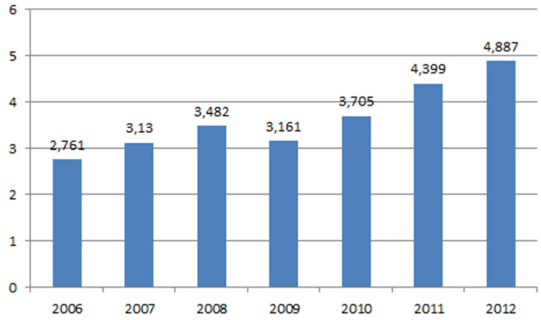


Figure 3 shows above the change of volume in USA B2B e-commerce between 2006 and 2012. In 2006 volume is 2.761 billion dollars. Everyyear volume is incresing except to 2009. In 2012 volume is 4.887 billion dollars. It is approximate increase %200 according to 2006[5].

2.1 Security issues in B2B Transactions

The issue of security has been a major barrier in the adoption of B2B e-commerce right from the beginning. The B2B e-commerce applications are exposed to various security vulnerabilities that affect the participation levels. The vulnerabilities or security threats like virus. News of security attacks on an organization's website depict the non-serious attitude organization and result in loss of reputation and loss of credibility.

In the Dell Security Research, saw POS malware variants and attacks targeting payment card infrastructures.Dell saw a rise in POS attacks attempted among Dell SonicWALL customers as well[6].

In the Cisco Security Research, in recent years, Java has played an unwanted starring role in lists of the most prevalent and severe vulnerabilities to exploit. However, Java appears to be falling out of favor among adversaries searching for the fastest, easiest, and least detectable ways to launch exploits using software vulnerabilities, according to Cisco Security Research[7].

2.2 Existing Solutions for Data Security in B2B Transactions

This section discusses the existing cryptographic solutions proposed by companies to enhance organizational data security.The figure 4 below indicates the proposed cryptographic solutions to enhance data security in B2B transactions.

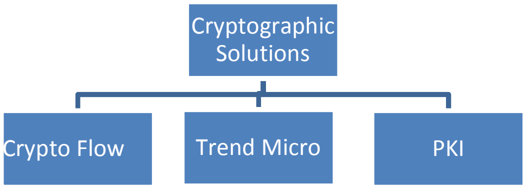


Figure 4. Existing Cryptographic Solutions

2.3 Cryptographic Data Security Solutions for B2B Transactions

Companies use the some methods for data security. These are Crytography and encryption. Example of possible solutions ; CryptoFlow, Trend Micro and PKI.*" Now with CryptoFlow B2B, enterprises can safely extend applications to external business partners, supply chain members and contractors without opening a major attack vector to hackers" (Solutions For CryptoFlow Notes).* Trend Micro Encryption provides an integrated portfolio of e-mail encryption services based upo. PKI (Public Key Infrastructure) data / information and communication in the public key that allows cryptography to be widely used and safe, and key generation working in coordination with each other, key management, approval agencies, digital notary public, covers all services such as time stamp.

Cryptography and Encryption

Privacy is handled by encryption. In Public Key Infrastructure (PKI), a message is encrypted by a public key, and a decrypted by a private key. Public key is distributed, but only the recipient get the private key. For authentication the encrypted message is encrypted again with a private key. Only sender has the special key. Because for identify the sender. This way is create RSA(used by banks and governments) and PGP(Pretty Good Privacy,used for encrypted emails).

Cipher systems are classified into 2 classes which are:

1- Secret key cipher system.

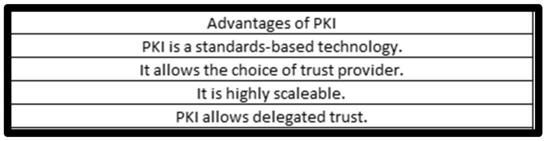
2- Public-key cipher system

Secret Key:
Secret key is the oldest type cryptography method. It has two main types which is transposition and substitution. Transposition cipher, encrypt the original message by changing characters order. Substitution cipher, encrypt the original message by replacing their characters with other characters. In both types sender and receiver is share the same secret key. Today is most of use secret key which is Data Encryption Standard (DES).DES cipher work with 56-bit secret key and 16 rounds to transform a block of plaintext into cipher text[8].

Public-Key Cipher System
Public-key cryptography is used to encrypt and decrypt a message so that is arrives securely. First of all, network user get a public and private key from authority. If other user wants to send an encrypted message can get the purpose recipient's public key from a public directory. They used this key for encrypted to message, and they send to recipient. When recipient get the message, they use the this key for decrypt to data. Otherwise no one cannot open the message[9].

2.3.1 PKI Cryptography

A Public Key Infrastructure (PKI) is the key management environment for public key information of a public key cryptographic system. PKI purpose is to allow the distribution and use of public keys and digital certificate to provide secure communication. In PKI, one key it is used for encrypted and decrypted the data and other key is used to perform the reverse operation[10].



Advantages of PKI
PKI is a standards-based technology.
It allows the choice of trust provider.
It is highly scaleable.
PKI allows delegated trust.

Table 1. Advantages of PKI

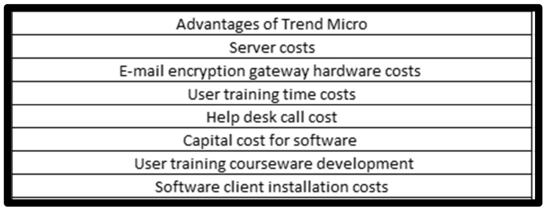
In this table, explain the advantages of PKI. It has five main advantages.

Disadvantages of PKI

They key size increases, so the data encryption and decryption time is increase." *While generating the key pair care should be taken to choose a high exponent value. The greater the exponent size the more secure the key is. If the exponent size is not specified during key generation most of the tools default to 3. The message encrypted with a key of exponent size 3 can be easily decrypted as below Message = (Encrypted message)^1/3.*[11]"

2.3.2 Trend Micro IBE

Trend Micros is designed for e-mail encryption. Its purpose easy user registration, simplify business processes and offload key management tasks to the cloud[12]. At the same time it can help financial benefits. The total cost of a typical PKI-based e-mail encryption solution cost is more than four times as much as a Trend Micro Encryption alternative.



Advantages of Trend Micro
Server costs
E-mail encryption gateway hardware costs
User training time costs
Help desk call cost
Capital cost for software
User training courseware development
Software client installation costs

Table 2. Advantages of Trend Micro
In this table, explain the advantages of Trend Micro. It has seven main advantages.

Disadvantages of Trend Micro IBE

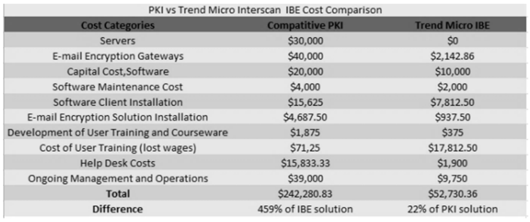
It has two main disadvantages." *First, the PKG has a master secret key, which if compromised would allow an attacker to decipher any message from any user. Second, the security of IBE relies on problems that have not been studied as extensively as the problems that underlie more traditional cryptosystems.*[13]"

2.3.3 Trend Micro IBE (Identity-based) vs. PKI Cryptography

Nowadays, large organizations exchanges to sensitive, private and regulated data with e-email. So E-mail security is very important for these organizations. Organizations need to e-mail encryption. Without encryption, this data free and clear on the Internet. But many organizations does not use the e-mail encryption, today's e-mail encryption is very complex. Currently, organization understands to important privacy. Fortunately things are changing. These are following;

Currently e-mail encryption methods are at the heart of the problem. End-to-end e-mail encryption methods are supported with PKI infrastructure. This is implementing a PKI back-end and distributing, managing digital certificates for each registered user. For IT organizations, PKI is expensive and not useful.

Identity-based encryption (IBE) can be effective alternative. Key management does not have to be complex. With IBE new methods does not need for digital certificates by calculating key values based upon identity characteristics like recipient's e-mail address. Other benefits of PKI without researcher's and PhDs to use it.



PKI vs Trend Micro Interscan IBE Cost Comparison

Cost Categories	Compatitive PKI	Trend Micro IBE
Servers	$30,000	$0
E-mail Encryption Gateways	$40,000	$2,142.86
Capital Cost,Software	$20,000	$10,000
Software Maintenance Cost	$4,000	$2,000
Software Client Installation	$15,625	$7,812.50
E-mail Encryption Solution Installation	$4,687.50	$937.50
Development of User Training and Courseware	$1,875	$375
Cost of User Training (lost wages)	$71,25	$17,812.50
Help Desk Costs	$15,833.33	$1,900
Ongoing Management and Operations	$39,000	$9,750
Total	$242,280.83	$52,730.36
Difference	459% of IBE solution	22% of PKI solution

Table 3. PKI vs. Trend Micro Comparison

The Figure 1 above indicates the comparison between PKI and Trend Micro systems. Trend Micro Encryption is primary alternative. IBE, solutions greatly basic key management, but some items still need users to manage key server and negotiate key exchange with external parties. Trend Micro Encryptions is an exception to this rule; it supports its premise-based e-mail encryption customers and gateways with cloud services for key management, and external user enrollment. This is the most important advantage to Trend Micro Encryption and efficient e-mail encryption today[14].

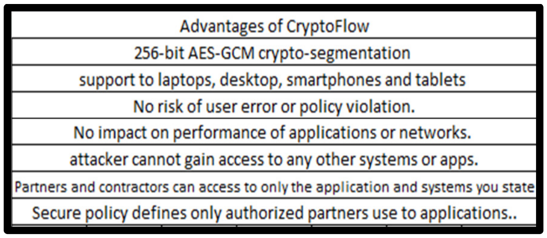
2.3.4 CryptoFlow

CryptoFlow offer interruption point and click security of data traffic for sensitive application across any network. Now with CryptoFlow B2B is developing for organizations can safely extend to data or applications to external contractors without a any attack vector to hackers. CryptoFlow is the first application-aware and user aware solutions for safeguard networked applications of this industry's. *"CryptoFlow B2B extends any networked application to external partners and automatically enforces cryptographically protected access to only the applications they need based on their roles."(Solutions For CryptoFlow Notes).*

Traditional security models, only safe as your partners. Because it is a perimeter based model. In this model focuses on granting access through the firewall for the external contractors and partners. But it has a any breached, credentials or any attack from the hackers, they gain the same unfettered access to your internal systems.

CryptoFlow for interrupt to application the reduces attack risk of extending access to partners. CryptoFlow B2B provided access permission to application only your authorized partners. Interruption is end-to-end, from data center or Cloud to the authorized external user and their registered devices.

Advantages of CryptoFlow



Advantages of CryptoFlow
256-bit AES-GCM crypto-segmentation
support to laptops, desktop, smartphones and tablets
No risk of user error or policy violation.
No impact on performance of applications or networks.
attacker cannot gain access to any other systems or apps.
Partners and contractors can access to only the application and systems you state
Secure policy defines only authorized partners use to applications..

Table 4. Advantages of CryptoFlow

CryptoFlow to eliminate hard-to-manage encryption technologies and traditional network segmentation which was designed for routing and not security. In CryptoFlow you have a single point of control to protect data from application to user any network (LAN, WAN, Wireless, Internet etc.) inside or outside. *"You are no longer dependent on firewalls or routers that are cut to a quarter of their performance level when encryption is turned on."*

CryptoFlow is a service provided in 84 countries around the world. It is used by financial institutions, healthcare networks, governments, multinationals and many others [15-16].

3. Comparison of Cryptographic Data Security Solutions

Trend Micro IBE is the cheapest model between this models. Also it is not complex, for user easy to understand. Its purpose easy user registration, simplify business processes and offload key management tasks to the cloud. This is implementing a PKI back-end and distributing, managing digital certificates for each registered user. It is expensive and not useful for the organizations.

Table5. Comparison of Cryptographic Solutions for B2B Data Transactions

	Advantages	Disadvantages
CryptoFlow	Decreased Costs High Speed Better Security	No Examined
Trend Micro IBE	Decreased Costs High Speed	Low Security
PKI Cryptography	Standards-Based Technology Good Security	Low Speed High Cost

Cryptoflow is the best model between these models. In the cryptoflow, no risk for user error or policy violations. Supporting any devices such as tablets, smartphones, laptops etc. It gives the services 84 countries around the world. Financial institutions, governments, healthcare networks used CryptoFlow.

4. Proposed theoratical Value Added Network (VAN) based Eelectronic Data Interchange (EDI) model to enhance organizational data security for B2B Transcations

Researchers have proposed variety of methods and techniques to enhance data transfer security in wired and wireless environments [17-25]. The literature covers variety of cryptographic methods and techniques used to enhance organizational data security [26-31]. The data security is essential for organizations that deal with the prevention of exchange of dignity and privacy of consumer's data. The electronic data interchange (EDI) uses node-to-node communication technologies in order to automate B2B purchases. The following theoretical EDI model is proposed to enhance organizational data security within an organization.

The proposed theoretical EDI model can replace even data encryption based transaction modules and security systems in case of deployment.

The methods proposed in the literature supports majority of the B2B transaction control models by including "Audit" mechanism and human takes place at this moment as an auditor. Audit has specific objectives to detect the unauthorized access to data, facilitate event reconstruction and promote accountability in case of any trouble. In such deployment mechanism, the audit have monitoring and reporting of security violations against organizational data security. The figure 5 below illustrates the role of an audit briefly.

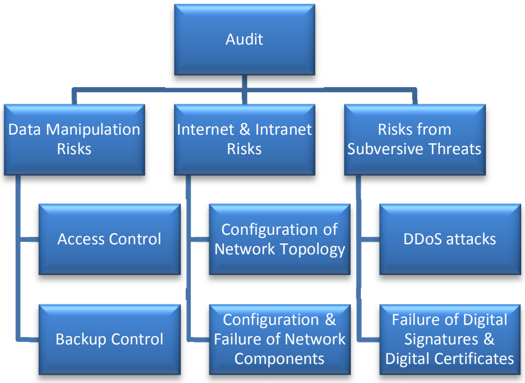

Audit
Data Manipulation Risks
Internet & Intranet Risks
Risks from Subversive Threats
Access Control
Configuration of Network Topology
DDoS attacks
Backup Control
Configuration & Failure of Network Components
Failure of Digital Signatures & Digital Certificates

Figure 5. B2B Transaction Control with Audit

Details of the Figure 4 are explained as the responsibilities of the Audit as follows;

a) Control of transaction authorization, validation and in compliance with the trading partner agreement,
b) To prevent Unauthorized organizations gain access to company's database
c) To control Authorized organizations to gain access to only authorized portion of data in database.
d) Responsible of configuration and deployment of the proper network topology,
e) Prepare the system and protect it against subversive attacks that may arise from outside or inside the company.

In order to support EDI environment with more secure infrastructure, the method can be Details of the Figure 5 are explained as the responsibilities of the Audit as follows; The theoretical EDI framework is shown in figure 6 below. The deployment model of the figure works on the basis of Value Added Network (VAN) which is supposed to be deployed separately to enhance organizational data exchange and support EDI. The Figure 7 illustrates the VAN infrastructure briefly.

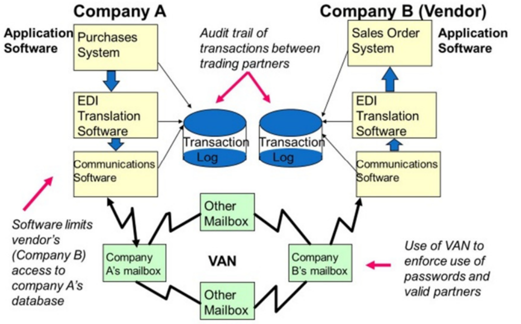


Figure 6 . Proposed VAN based Theoretical EDI Framework

The Company A and Company B exchange data where EDI translation software are deployed in both parties and integrated with companies purchase application systems. The corresponding transaction logs are recorded between trading parties through EDI. The communication software of EDI is setting limits complete access of company A to company B's database.

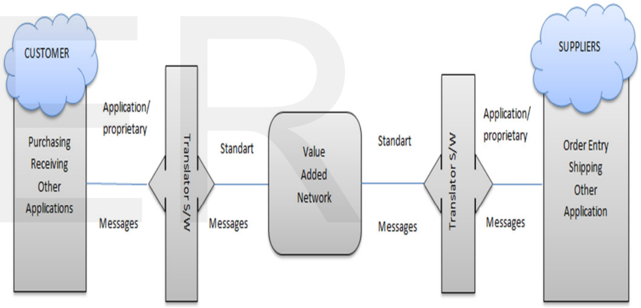


Figure 7. Value Added Network (VAN)

The figure 6 illustrates the VAN deployment above. VAN is a third party network that provides services to execute authorized transactions with valid trading partners using EDI mechanisms. In order to exchange data, the authorization and validation processes must be completed for VAN. The use of VAN ensures validation of the partners and creates a unique data exchange environment in terms of security. In addition to this, the usage of passwords, encryption mechanisms and chipertext can be enforced between business partners during exchange of data through VAN. In addition to that, since the process of data exchange would be on a separate platform such as VAN, it won't require any of the partners to deploy additional mechanism or infrastructure to enhance security during any sessions of the exchange of data transactions. The mail boxes used by both parties are encrypted in VAN and both parties' mails are exchanged in a separated mail server box. The VAN requires complete secure communication and forces both parties to use security enhanced messages to communicate with each other.

Conclusion

Nowadays, B2B type e-commerce transactions are increasing day by day and security becomes an essential factor for organizations that conducts these transactions through data transmission. This article proposed a new theoretical cryptographic model to solve security related data transfer issues during data transfers and compared three most popular cryptographic B2B applications used by B2B organizations such as CryptoFlow, PKI and Trend Micro. The comparative survey indicated that CryptoFlow is the most secured B2B application among all others since it uses 256-bit AES-GCM crypto-segmentation and provide special support for laptops, tablets, desktops and smartphone transactions. Trend Micro is the cheapest module between these modules while providing ease of use and less complex environment to end-users. In addition to this the efficient premise-based e-mail encryption for customers and gateways with cloud services for key management, and external user enrollment are additional features of Trend Micro application. The PKI shown lower performance in terms of pricing and encryption progress with complexity and not preferred by organizations and this results indicated that, the use of 256-bit AES-GCM mechanism is still popular among B2B companies to enhance data security. This research has compared the cryptographic data security solutions in B2B transactions by exposing a new theoretical model for companies to deploy and researchers to conduct a deployment experiments on them. The proposed theoretical EDI mechanism does not require any human to involve into electronic interchange so it eliminates subversive attacks to data where the physical infiltration may arise. The prevention of physical intervention will increase the effectiveness and efficiency of the overall system. This model can be deployed successfully for the B2B transactions to enhance organizational data security or further researches can be carried out to expose possible practical deployment models.

References

[1]JBV Subramanyam, Kokula Krishna Hari K. ,The Proceedings of the International Conference on Information Engineering, Management And Security 2014 (ICEMS 2014) VOLUME 1 P.117

[2]Wienclaw R., (2015) "B2B Business Models", Research Starters Business, p.1, 1/1/2015, EBSCO Publishing Inc.

[3]Sari, A. and Akkaya, M. (2015) Security and Optimization Challenges of Green Data Centers. International Journal of Communications, Network and System Sciences, 8, 492-500. doi: http://10.4236/ijcns.2015.812044.

[4]Statista Dossier (2015) "B2B marketing in the U. S.", March 2015.
Available at:
https://www.ama.org/publications/eNewsletters/Marketing-News-Weekly/Documents/ama-weekly-download-b2b-marketing-in-the-us-dossier.pdf
Page: 9 Last accessed: 16/12/2015

[5]Statista Dossier (2015) "E-commerce in China", The Statistics Portal, November 2015.
Available
at:http://www.statista.com/study/11567/e-commerce-in-china-statista-dossier/

[6]2015 Dell Security Annual Threat Report Year: 2015 Available at:
http://www.sonicwall.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf Last accessed: 16/12/2015

[7]2015 Cisco Security Annual Threat Report Year: 2015 Available at:
http://www.cisco.com/assets/global/UK/solutions/executive/security/pdf/Cisco-2015-ASR-Executive-Summary-EN.pdf Last Accessed: 16/12/2015

[8]William Stallings, ―Cryptography and network Security‖,4th edition, Prentice Hall,2005.

[9]Burt Kaliski, "The Mathematics of the RSA Public Key Cryptosystem", RSA Laboratories. April 9, 2006. Available at: http://www.mathaware.org/mam/06/Kaliski.pdf Last accessed: 16/12/2015

[10]Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Tech-niques in Wireless Networks. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 567-577. Doi: http://dx.doi.org/10.4236/ijcns.2015.813051.

[11]By Joel Weise - SunPSSM Global Security Practice Sun BluePrints™ OnLine - August 2001, Public Key Infrastructure Overview, Available at: http://www-it.desy.de/common/documentation/cd-docs/sun/blueprints/0801/publickey.pdf Last accessed: 17/12/2015

[12]A Dell Technical White Paper, Public Key Infrastructure in iDRAC Available at: http://media.community.dell.com/en/dtc/attach/idrac6%20pki%20white%20paper.pdf Last accessed: 17/12/2015

[13]Trend Micro™, Encryption for Email Client, Available at: http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_email_encryption_client.pdf Last accessed: 17/12/2015

[14]Journal of Research of the National Institute of Standards and Technology, Report on Pairing-based Cryptography, Volume 120 (2015) Available at: http://dx.doi.org/10.6028/jres.120.002 Last Accessed: 17/12/2015

[15]Sari, A. and Karay, M. (2015) Comparative Analysis of Wireless Security Protocols: WEP vs WPA. International Journal of Communications, Network and System Sciences, Vol. 8, No.12, pp. 483-491. doi: http://10.4236/ijcns.2015.812043.

[16]Oltsik, J. (2010), "The True Costs of E-Mail Encryption", Enterprise Strategy Group, White Paper, June 2010, Available at: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_true-costs-of-email-encryption_analyst-esg.pdf.

[17]Solution Note CryptoFlow B2B Available at: http://certesnetworks.com/pdf/solution-notes/solution-note-cryptoflow-LAN.pdf Last accessed: 16/12/2015

[18]Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 http://doi.acm.org/10.1145/2523514.2523586.

[19]Sari, A. (2014); "Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS", International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: http://dx.doi.org/10.4236/ijcns.2014.79038.

[20]Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 533-542. http://dx.doi.org/10.4236/ijcns.2015.813048.

[21]Sari, A. (2014); "Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks", Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: http://dx.doi.org/10.14738/tnc.25.431.

[22]Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". International Journal of Communications, Network and System Sciences, Vol. 8, No.3, pp. 19-28. doi: http://dx.doi.org/10.4236/ijcns.2015.83003.

[23]Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". International Journal of Communications", Network and System Sciences, Vol.8, No.3, pp. 29-42. doi: http://dx.doi.org/10.4236/ijcns.2015.83004.

[24]Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative

Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", New Threats and Countermeasures in Digital Crime and Cyber Terrorism, (pp. 66-94). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7. April 2015.

[25]Sari, A. (2015) "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security", Vol.6, No.2, pp. 142-154. doi: http://dx.doi.org/10.4236/jis.2015.62015.

[26]Obasuyi, G. and Sari, A. (2015) "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. International Journal of Communications, Network and System Sciences", Vol.8, No.7, pp. 260-273. doi: http://dx.doi.org/10.4236/ijcns.2015.87026.

[27]Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 471-482. doi: http://10.4236/ijcns.2015.812042.

[28]Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Net-works (VANET). Int. J. Communications, Network and System Sciences, Vol. 8, No.13, pp. 552-566. http://dx.doi.org/10.4236/ijcns.2015.813050 .

[29] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.) Network Security Attacks and Countermeasures (pp. 270-312). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8761-5.ch012

[30]Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, http://dx.doi.org/10.1109/CICSYN.2013.79 .

[31]Sari, A., Onursal, O., (2013); "Role of Information Security in E-Business Operations", International Journal of Information Technology and Business Management, Vol.3, No.1, pp. 90-93, ISSN: 2304-0777.