Centralized Solution to securely transfer Payment Information electronically to banks from Multiple Enterprise Resource Planning (ERP) Systems

Manu Kohli
School of Informatics and Computing
Indiana University Bloomington,USA
Email: kohlim@umail.iu.edu

Edgardo Suarez
Kelley School of Business
Indiana University Bloomington,USA
Email: tsuarez@earthlink.net

***Abstract*—Financial transactions in an organization, for example payments to suppliers and employee salaries, are generated from Enterprise Resource Planning (ERP) applications and require secure transmission to bank. The payment models have been evolving over the years which confronted transformations from the usage of manual payment methods, cheque, cards, Electronic Fund Transfer (EFT) to Automatic Clearing House (ACH). Current models utilize Public key infrastructure methods for authorization procedures which require certification and verification of customer and payment information. The present case study proposes a consolidated model that has been developed and deployed using a centralized infrastructure enabling secured payment information exchange from various business units in an organization to the bank. The developed method achieves economies of scale and scope, provides set of standardized procedures that integrate multiple ERP applications deployed for various business units distributed over multiple geographies on a secured platform at a minimum reconstruction and waiting time. The model has proven effective leading to cost and schedule saving from 25 % to 75% and provides a plug and play platform to business units in an organization to exchange payment information securely with various banks.**

Payroll Processing,SSH File Transfer Protocol(SFTP),data encryption,Automated Clearance Houses,ERP systems, Pretty Good Privacy (PGP)

I. Introduction

ERP applications are deployed in various industry sectors such as manufacturing, media, trading houses that utilize an automated payment framework through standard account payable module. The payment runs are executed either to process employee salaries or to make supplier payments. However, in larger firms, the volume of transactions and often the amounts in play are encountered at millions of dollars, hence safety and security to exchange the payment data with the bank becomes crucial. An increased complexity is observed in ensuring secured payment transmission to bank when organization is going through organic/ inorganic growth, resulting in transformation of its Information Technology (IT) landscape and maintaining secured payment infrastructure with partner banks. The complexity is further multiplied where different business units in an organization deploy varied ERP and IT applications to generate payment information that is exchanged with the bank.

The paper emphasizes on securing the payment data generated from one or more than one ERP applications and formalizing treasury approvals guidelines and constructing secured infrastructure on best practices. The consolidated centralized secured model,already developed and implemented, integrates multiple ERP applications across various business units spread out in multiple geographies to carry out banking transactions and exchange payment information securely with banks. The centralized infrastructure uses secured transmission methods to achieves economies of scale and scope and can be utilized in global frameworks at a minimum reconstruction and waiting time.

II. Literature Review

The extensive literature review highlights the need for securing payment transmission and making various associated procedures efficient. The inefficiencies prevalent in present payment applications and the evolvement of measures to reduce risks before payment is authorized are discussed widely in this study. The payroll payment involving confidential transactions needs to be encrypted to avoid fraudulent activities. Djuric [1] analysed the potential risk factors involved in payment processing and necessities the usage of cryptography techniques. Dharaiya et al. [2] insisted the need for encryption of data through cryptography to ensure high security. Usman and Shah [3] emphasized the requisites of internal control to prevent fraud occurrences and also to enrich the authentication systems.Coronado-Garcia et al. [4] and Babu et al. [5]has utilized public key infrastructure model to secure transactions.

Dharaiya et al. [2] analyzed ERP systems, which deal with sensitive data, require additional security measures and information from such systems needs to be encrypted for higher security. It is also necessary to detect frauds and intrusions at the right time in such systems. The security of the data has been enriched through usage of cryptography techniques. The study further has tried to identify the detection of fraudulent activities through event log tables. The transaction authorization limits and roles assignment as per segregation of duties can limit the risk of fraudulent activities.

978-1-5090-3584-7/16 $31.00 © 2016 IEEE
DOI 10.1109/ICIT.2016.56

Masocha et al. [6] identified few social and cultural issues hindering the development of e-transactions such as language barrier, cross cultural country legislation barriers, logistical barriers, limited access to internet, and few security concerns. Moreover, implementation of an integrated ERP system for a secure transmission demands changes in existing organizational culture [7] since traditional transaction method may be prevalent in the geography of implementation.

Usman and Shah [3] analyzed and offered solutions for E-banking fraud. Frauds in e-banking services occur as a result of various compromises in security ranging from weak authentication systems to insufficient internal controls.

The purpose of this paper is to understand factors that could be critical in strengthening fraud prevention systems in electronic banking. The study findings show that beyond technology, other factors such as strengthening internal controls, reusing technology infrastructure and standardizing treasury framework to approve payments can secure payment information to bank.

Coronado-Garcia et al. [4] analyzed Public Key Infrastructure (PKI) and its essentiality to assure secure transactions and high reliability of its services. The use of public key cryptography satisfies the first requirement, while the second requirement has been traditionally satisfied by the use of distributed architectures. Babu et al. [5] considered rapid increase in Public Key Infrastructure (PKI) enabled applications in various electronic transactions, it has become very important to audit the deployed PKI System regularly and to understand the effectiveness of the system. The researcher proposed an agent-based approach to audit a PKI System. This system utilized a certificate generated life cycle on authorization procedures. The agent based approach offered effective audit reports for a public Key infrastructure that was more effective than the manual audits.

The analysis of previous literature has provided certain challenges in the payment process which have been listed below. The proposed centralized infrastructure to transfer payment information securely to banks overcome the observed challenges.

III. Challenges Faced By Existing Model

A. Fraudulent Activities during Payment Transactions

Firms that are utilizing ERP frameworks interchange their payment related data with the bank. The information exchange with the bank is done using a file that includes payment details, amount, currency and the bank account credentials. At most of the times this data transferred is prone to fraudulent services by either modifying account number or the amount transferred [8].

B. Inefficient Manual Processing

Account payable division in an organization plays a critical role in exchanging payment information for suppliers or employees with bank. Payment process and subsequent approvals can be automated with the use of ERP applications and if carried out manually consumes significant time. Gate point Research by Tipalti [9], found that 72 respondents spend over five hours a week setting up payees, favouring and issuing payments, resolving payment related problems, and performing other conciliations associated with payments. The survey further accounted that 48% of respondents had either submitted payment reports manually to the bank or utilized information from ERP frameworks. After this process, data upgrading and updating becomes a manual task not only risking possibility of a fraud but also making data conciliation difficult. These manual procedures are prone to errors and misinterpretations.

C. Non Standardized Transactions through Payment Gateways

Four out of five firms are disclosing their activities to payment misrepresentation in view of an absence of standardized payment work processes [10]. The organizations with a high level of complexities suffer from proliferating operational and transaction expenses. Thus there is an expanded interest for controls, and it demands for a centralized infrastructure with secured base to exchange payment data to bank [10].

D. Multiple Banking Relationships and Transactions

The B2B Payments and Bank Connectivity faced issues with divergent frameworks of multiple ERP networks connecting transactions from various banks. The payment network is more intense and complex in multiple banking environments. The report by SunGard elucidates that this complexity has made 25% of organizations dealing their business transactions in excess of 10 cash management banks, 23% of organizations handling more than thousands of bank accounts [11]. Whereas 89% of the organizations have expanded their business activities across various countries, these international banking services are pooled to e-banking transactions for more than 55% of the activities which earns revenue of $1 billion. Out of the total transactions taken place internationally, 29% of the banking services has reported with data hacking, fraudulent services and misinterpretation of data [11]. The opportunities for data security and accurate interpretation are not recognized by the organizations so as to mitigate the security threats.

IV. Various Payment Modes

The major payment methods are electronic cheques, Automated Clearance Houses (ACH), and Electronic Fund Transfer (EFT) [12]. The study conducted by SunGard on B2B payments on analysing 400 treasury and financial experts evidenced that 15% of the respondents are utilizing paper cheques rather than other prevalent payment methods such as electronic credit / debit cards, ACH and EFT. The organizations still utilizing cheques are facing critical risks of fraud activities [11]. The figure 1 depicts the share of prominent usage of payment methods.

A. Cheques

A survey analysis conducted by the Association for Finance Professionals identified Cheques are the prominent payment methods subjected to fraudulent activities representing the

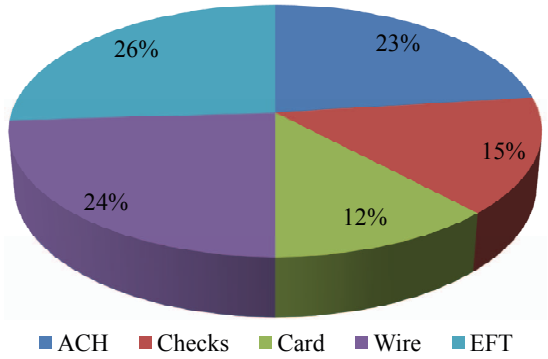

Fig. 1. Most Popular Payment methods [11]

biggest dollar amount which was accounted on loss in 2014. To combat these losses, banking relationships have started rationalizing and transforming into digital solutions on a slower pace [13]. The minimized usage and reliance on cheques reduces the misinterpretations and frauds in manual processes [14].

Positive pay is an automatic detection tool incorporated by leading banks for detecting fraudulent activities by validating the account number, fund details, cheque numbers against a list of authorized cheque numbers issued by the bank.

B. ACH

ACH exercises control over the consistency of payment flows and reduces check misrepresentation by utilizing ACH records to process payment to their employees, merchants, and other associated stakeholders. ACH handles vast volumes of credit and debit transactions [15].

C. EFT

A solitary electronic payment file trades with multiple payments by consolidating different ERP systems and various EDI formats.

V. Security in File Transmission

The financial payment transaction initiates from an ERP application by an account payable department of an organization requiring to exchange funds with another business entity or organization with bank as an intermediary. The file that is exchanged with bank should be encrypted and should be generated after approval of the payment by the responsible person as per the delegation of authority defined in an organization. The person authorized to carry out financial payment transactions or approvals may take additional time and scrutiny in performing approval. If the time exceeds certain limit, the financial transaction may fail to initiate or a delayed approval process may cause the in process payment to be denied [16].

A. Methods of Preventing Payment Risks

The following methods listed below can reduce fraud during transfer of payment information to bank.

- Avoiding or minimizing usage of paper to seek approval or exchange payment information.
- Improving and emphasizing authority via an established 'segregation of duty' process to access data and approve payment issuance on clearly defined delegation of authority roles.
- Usage of automated payment system where human intervention can be avoided to access the payment file that is exchanged with the bank
- Characterizing an approval methodology for e-Payments as last step on bank portal once file is received by the bank.The approval necessitate formal agreement between treasury department and the bank to release payment to the beneficiary as stated in the payment file.

In order to overcome these issues presented, the study proposes a model that is already developed and implemented to handle transmission of e-Payments with various banks on a secured platform.

VI. Proposed Model

The payment file shared securely with the bank ensure no fraud or misrepresentation can happen on the transacted financial data. The present study proposes a centralized infrastructure model to accommodate various business units utilizing multiple IT applications to perform banking transactions. The centralized infrastructure operates in harmony with various organizations, follows general guidelines for treasury management and a specialized technical infrastructure to impart the payment information amongst the banks. The infrastructure is framed to achieve the subsequent guidelines.

- A solitary policy for payment endorsement and approvals, signing and to release the payment incorporated in the ERP application.
- Payment approval process designed on best practices as per organization's treasury guidelines.
- Release of payments to banks in consistence with organization commands on sum seethes, financial balances and elements for marking and endorsement.
- Data seals to anticipate messing around with payments information
- Secure interfaces to and from ERP frameworks for the trading of scrambled and marked records
- Secure and value-based keeping money channels that counteract messing around with payment records.
- Processing history and audit trails incorporating all payment handling steps, including time stamps, clients and changed properties
- Final approval of payment on the banking portal once the payment information is successfully exchanged with banks.

She and Thuraisingham [16] has validated the payment processing models involving security with authentication tech-

niques involved in transmitting the data. The automated payment procedure through this framework ensures avoidance of manual intervention in payment process, thereby reducing the risks to altering the file or triggering fraudulent activities. Encryption of data and secured connectivity measures in the payment process includes utilizing keys and certificate verification and revalidation to exchange and interchange payment information across various gateways. This ensures security and elimination of fraud when payment information is exchanged with the bank.

A. Features of Automated Payment Systems

Irrespective of the process dealt with payment systems, the organization ought to utilize this secured infrastructure which is formulated with specific features such as:

- Secured system ensuring correct definition and assignment of roles as per established delegation of authority and segregation of duties.
- Automated procedure i.e., no manual access to the payment file to minimize risk of fraud or misrepresentation that can happen by changing the payment details after the payment data is generated from the ERP application.
- Secured development to transfer payment information file via automated scripts from an ERP application to bank.
- Once the payment file is sent to bank, an affirmation of the payment data is sent to capable individuals in the association. An extra security highlight is recommended to be fused where once the payment data is received by the bank, a capable individual can logon to the bank entry and can approve, witness and favor the payments.
- Quick Adaptability allowing the solution to be reused with minimum waiting time.

B. Automated Payment Infrastructure

The increase in transactions has made the audit departments of corporate offices handling customer accounts in a critical situation to review the payment flows and also to identify the possibility to fraudulent activities. Prior to the initiation of payment transaction processes, the files related to accounts are made accessible to the treasury in an ERP system. Chances of threats to data theft are witnessed since the data has been stored in an ERP system or on a network for a longer time period even before the initiation of the transaction. The most suitable approach is to maintain a strategy to eliminate fraud through completely computerizing the procedure, not using paper payment approvals and also intending to limit utmost the time period of data stored temporarily during transaction processes on paper or an unsecured network directory.

The present model considers a fully automated structure with high degrees of control through encrypted data which connects various banks and business entities through a single and secured network. Usually SWIFT Net technology is adopted to link treasury and corporate financial structures within a defined corporate environment. In the absence of SWIFT Net or banking financial systems an encrypted SFTP protocol is used for secured transfer of data and files. In case an SFTP is available the automated process directly exchange payment data with bank avoiding any manual access and possibility of fraud.

The security is enhanced by means of generating a file automatically on network where any individuals are prohibited to access the data. This secured framework requires robust verification in terms of error free handling and is completely automated. The secured transactions of payments and the exchange with the bank is done in a three step process as shown in Figure 2. The three step process takes care of all the payment process related to payroll or supplier payment in an organization.

STEP 1 - Automated Payment generation: Payment run is carried out by the accounting department using enterprise resource planning (ERP) application and payment information file is generated and saved automatically at a secured server, the access to which is controlled with limited authorization.

STEP 2 Secured file transfer through data encryption: In this step files are transferred periodically, usually every 10 minutes, using a scheduled job and a SSH File Transfer Protocol (SFTP) connection to an encryption server.

Secured File Transfer Mechanism: The push and pull of files are executed through specific scripts via SSH File Transferred Protocol (SFTP) connection requiring file to move through various gateways. The connection between various local business units and centralized encryption server and finally with the banks is established through a SFTP. The directory definitions between various units and centralized encryption server are smartly defined and harmonized to ensure that the data transfer between business units and the secured Infrastructure is uninterrupted and clearly tracked. The infrastructure allows both push and pull as both the ERP applications and file encryption server is located in an organization network. To ensure an additional security layer a secured file transfer system is established (with a combination of private key a public key) depending which party if either pushing or pulling the data.

SFTP is a network protocol that provides file access, file transfer, and file management over any reliable data stream. The SFTP protocol allows for a range of operations on remote files which make it more like a remote file system protocol. The benefits of using SFTP protocol include resuming interrupted transfers, directory listings, and remote file removal. The security of the SFTP protocols are enhanced through utilizing subsystems of SSH protocol version in two stages. The SFTP server on SSH 2 protocol is not an independent platform and hence a client willing to connect with SSH 2 server needs to be aware of the path connecting SFTP server. The user authenticates the protocol with a private / public key and the usage of private key is limited to the user alone. The server connecting to user has a copy of the public key and when the user logged in with private key, the server challenges the user through an encrypted public key through an accessible directory . The private key of the user has the ability to decrypt the key sent by server and thereby providing the access.

For further security, the payment file is encrypted using

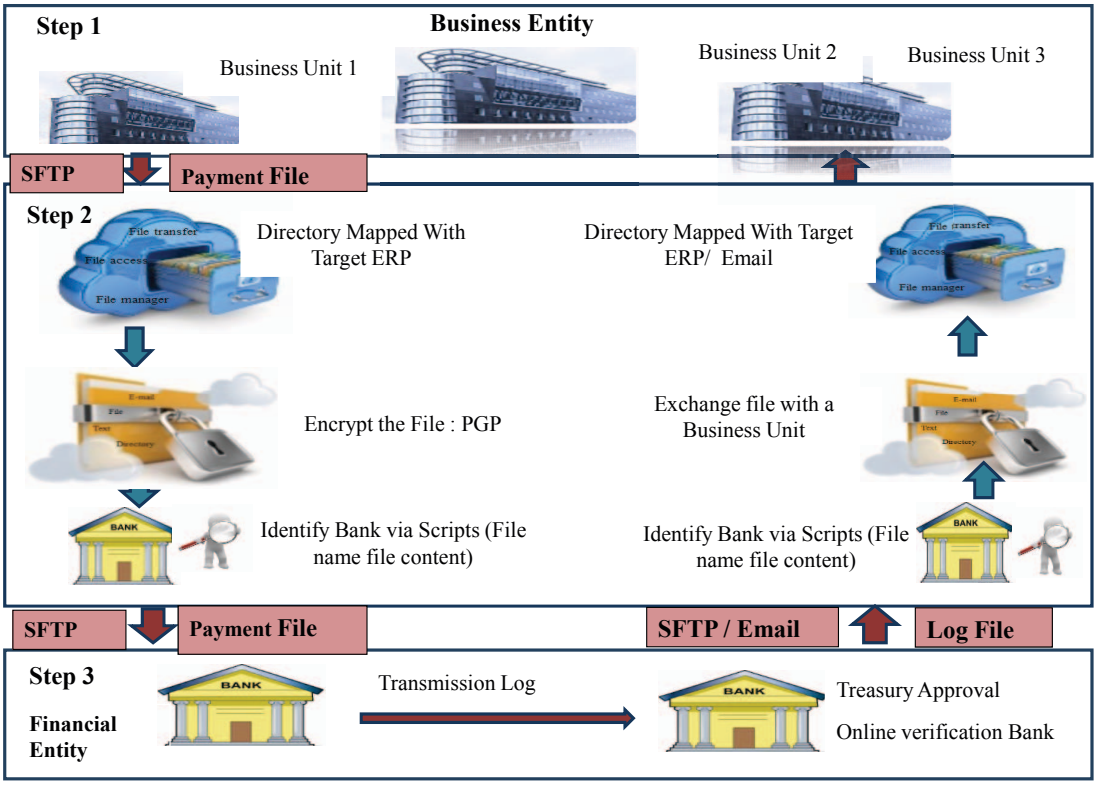

Fig. 2. Centralized solution for integrated various ERP for a secured financial transaction

industry based encryption standards such as Pretty Good Privacy (PGP). Most of banks use and accept PGP encryption methodology.

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. The keys computed for file encryption process once expire starts to regenerate automatically through certified verification. This certified system ensures the security in monetary transactions, business continuity, time saving and improved security. In the proposed model private encryption key is kept by the organization and the public key is shared with the bank. This additionally gives an improved layer of security.

STEP 3 Transferring File to the bank, payment log and Treasury approval:

In this step payment information file is transferred to the bank and additional approvals from the organization treasury are sought directly on the online bank portal.

The process initiates with file encryption after which they are routed to the bank. However, a business unit may be working with one or more than one bank. The scripts are designed or can be reconfigured to identify files destination (bank / business units) based on name or content and are routed to a gateway that transmits files to the bank at regular time intervals. The files transfers to bank are completely automated using host to host transfer protocol.

Usually if an organization is working with a single bank the secured connection already exists and can be scaled up quickly for other entities and business units that may want to transact with the same bank. The connection with the bank can be extended for other entities using the smart definition of the payment files. The model thereby provides an incentive to consolidate bank accounts and banking partners realizing reduced overheads and operating costs specially when an organization is going through process of mergers and acquisitions.

The developed solution is capable of handling varied payment methods, standardize treasury guidelines and define template based delegation of authority rules in ERP application as per organization / business unit policies. The infrastructure thereby offers itself as a standardized solution that harmonizes the security of the payment process generated from multiple business units and ensures that with no manual intervention payment information is shared with the bank.

Log file management: Once the files are routed to the bank it is possible to request the processing log information from the bank to confirm if the file is processed with no errors. The log file can be routed to a distribution list in the business entity for cross validation and taking corrective action in case of master data errors.

C. Observance of implementation time for the model

The proposed model consumes time for setting up the connection between the first entity and the bank however the time required for setting additional connections for business units or entities joining at later stages is exponentially reduced. The time lines recorded in table 1 and table 2 were observed during implementation of the model in America region where multiple business units in an organization from United States, Canada and few countries from South America were part of deployment. The model implementation was extended to another group company and was tested successfully on similar observed time lines having various entities in North America, Europe and Asia.

The time lines mentioned in the table below are limited to technical evaluation, technical discussions including testing and subsequent technical implementations to build the secured infrastructure. The time required in hours for setting up the connection for the first time and then extending it for the subsequent entities is listed in table 1 and graphically represented in figure 3. Table 2 and Figure 4 represents the comparison of exploratory and technical cost along with the implementation time lines during the set up of first connection and subsequent connections. The exploratory cost is a sum of time spent by a business unit in exploring and evaluating best possible technical solution to exchange payment information with the bank and finalizing payment process and administrative procedures with the partner bank .The time taken to implement technical solution for an entity is considered as a technical cost for analysis.

TABLE I
TIME DISTRIBUTION TO SETUP MODEL (HOURS) AUTHOR, 2016

	1st Entity	2nd Entity	3rd Entity	4th Entity	5th Entity
Exploration	70	50	35	25	25
SFTP between ERP (Step 1) and Business units	120	15	15	14	13
Encryption PGP (Design and test)	75	8	8	8	6
Scripts to scan the files	15	4	4	3	3
Discussion with Banks (Including tests)	120	70	48	32	32
Solution development	15	8	6	6	6
Infrastructure Maintenance	5	1	1	1	1
Security Approval	5	1	1	1	1
Provisioning of servers	4	1	1	1	1
Total Hours Required	429	158	119	91	88

Usually setting up any new file transmission process between a business entity and bank along with defining treasury guidelines consumes certain amount of down time that can vary from 2 months to 1 year. The time is spent carrying out extensive evaluation process and solution feasibility discussion with banks and internally within the IT organization. However, through the proposed infrastructure down time can be minimized as the infrastructure is readily available. This is very critical in case of organization going through restructuring and mergers and acquisitions process.

TABLE II
COST INCURRED FOR SETTING UP THE CONNECTION(AUTHOR, 2016)

	Exploratory Time (Hours)	Technical Time (Hours)	Total Time (Hours)	Implementation time lines (Months)
Entity /Business Unit 1	190	239	429	180
Entity /Business Unit 2	120	38	158	45
Entity/Business Unit 3	83	36	119	45
Entity/Business Unit 4	57	34	91	45
Entity/Business Unit 5	57	31	88	45

Table 2 represents the fact that total time incurred in setting the connection is higher for the first entity but once the proposed model is expanded to various geographies, the principle of learning curve theory and scalability brings in efficiency and the implementation time decreases. The decrease in implementation cost and improvement in solution implementation time lines is represented graphically in Figure 4. Here cost is considered directly proportional to time and is represented as exploratory and technical cost.

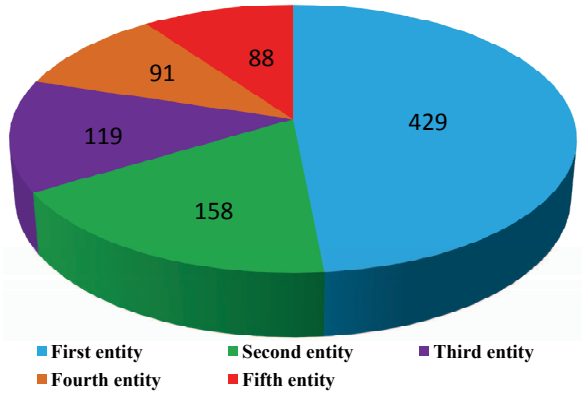

Fig. 3. Total Hours required for Setting up Transactions (Author, 2016)

D. Benefits observed with the implemented model

The proposed model integrates multiple ERP applications on a secured infrastructure to exchange banking transactions and offers various quantifiable and qualitative benefits over the public key infrastructure models. The exploration time for setting up a connection is reduced and so is the technical implementation time for the 2nd entity onwards as shown in figure 5. Moreover the learning from the project implementations are extended to new entities that reduces the project implementation time to 25% for any new entity joining the

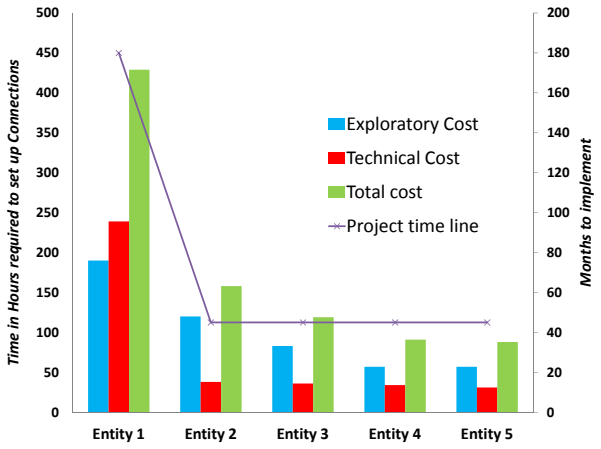

Fig. 4. Cost savings over the project time line(Author, 2016)

platform. The benefits of security infrastructure and treasury guidelines once implemented can be reused by new incoming entities or business units that become part of the model.The security threats are minimized as the entire framework operates within the firewall of the organization and payment data file is encrypted using private key that is held with the organization

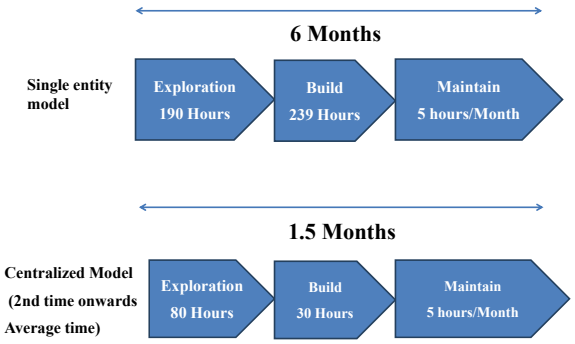

Fig. 5. Cost and schedule benefits of Centralized model for payment transfer(Author, 2016)

The model described thus manages data security (via an encryption factory), achieves economies of scale and can be replicated for various business entities across different geographical regions with standardized processes but allowing region specific legally required modifications. The model also achieves economies in terms of scope since the same solution can be incorporated during expansion of territories in business through mergers and acquisitions with a minimum down time.

The secured model technically integrates various ERP applications for different business entities by ensuring the appropriateness in terms of naming the payment file and folder structure to distinguish each entity and bank. The secured connection between SFTP and ERP systems once created and established, can be reconstructed for a new incoming business entity and its ERP system with no waiting time. Maintenance of the IT frameworks after implementation does not consume much time and the cost is distributed for every new entity joining the secured platform.

VII. Conclusion

The proposed centralized infrastructure model integrates various ERP applications used by multiple business units within an organization on a secured platform to exchange payment information with bank. The usage of secured file transfer protocol and encryption technologies on central infrastructure enables secured file transmission to the bank. Further, the solution supports the banking transactions and transmits instructions regarding payments through an Automated Clearance House or positive pay in a secured procedure by avoidance of fraudulent activities. The information passage across the banking completes its loop by exchanging standardized information with possibility of customization across multiple business entities. The model allows significant cost savings, agility to adopt local treasury guidelines and negligible downtime to extend the solution technically to a new entity or a business unit.

References

[1] Z. Djuric, "Ips secure internet payment system," in *International Conference on Information Technology: Coding and Computing (ITCC05)*. Canada: IEEE, 2005, p. 425 430.

[2] K. Dharaiya, K. Shah, A. Lokegaonkar, and S. Jadhav, "Fraud detection and security for erps with sensitive data," *International Journal for Innovative Research in Science & Technology*, vol. 1, no. 10, pp. 261 – 262, 2015.

[3] A. Usman and M. Shah, "Critical success factors for preventing e-banking fraud," *Journal of Internet Banking and Commerce*, vol. 18, no. 2, pp. 2 – 14, 2013.

[4] L. Coronado-Garcia, C. Hernandez-Lopez, and C. Perez-Leguizamo, "A uniqueness verifying public key infrastructure based on autonomous decentralized system architecture," in *International Symposium on Autonomous Decentralized Systems*. Athens: IEEE, 2009, pp. 1 – 6.

[5] P. Babu, M. Sivakumaran, and N. Dhavale, "Auditing public key infrastructure systems: An agent based approach," in *World Congress on Nature & Biologically Inspired Computing (NaBIC)*. Coimbatore: IEEE, 2009, pp. 1632 – 1635.

[6] R. Masocha, N. Chiliya, and S. Zindiye, "E-banking adoption by customers in the rural milieus of south africa: A case of alice, eastern cape, south africa," *African Journal of Business Management*, vol. 5, no. 5, pp. 1857 – 1863, 2011.

[7] M. Srivastava and B. Gips, "Chinese cultural implications for erp implementation," *Journal of technology management & innovation*, vol. 4, no. 1, pp. 105 – 113, 2009.

[8] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack two-factor authentication internet banking," in *17th International Conference*. Berlin Heidelberg: Springer, 2013, p. 322 328.

[9] C. Amit. (2016) 4 reasons to automate your ap processes. [Online]. Available: http://www.itproportal.com/2016/02/05/4-reasons-to-automate-your-ap-processes/

[10] E. Holley. (2014) Corporates taking too much payment risk warns sungard. [Online]. Available: http://www.bankingtech.com/219602/corporates-taking-too-much-payment-risk-warns-sungard/

[11] SunGard. (2014) Sungard b2b payments and bank connectivity study: Innovations to overcome complexity-driven fraud exposure and cost increases. SunGard. [Online]. Available: https://www.sungard.com/solutions/corporate-liquidity/campaigns/Global-Connectivity-Messaging-Study-Whitepaper.aspx

[12] A. Phulia, M. Sharma, and D. Kumar, "Role of online banking in economy," *International Journal of Research*, vol. 1, no. 7, pp. 1039 – 1044, 2014.

[13] ACFE. (2010) Report to the nations on occupational fraud and abuse. ACFE. [Online]. Available: http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rttn-2010.pdf

[14] O. Sobko, "Fraud in non-cash transactions: Methods, tendencies and threats," *World Applied Sciences Journal*, vol. 29, no. 6, pp. 774 – 778, 2014.

[15] CEBP, *Business-to-Business EIPP: Presentment Models and Payment Options*. Herndon, VA: CEBP, 2001.

[16] W. She and B. Thuraisingham, "Security for enterprise resource planning systems," *Information Systems Security*, vol. 16, no. 3, pp. 152 – 163, 2007.