ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics and Information Engineering

Vol. 11, No. 1 (Sept. 2019)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 11, No. 1 (Sept. 1, 2019)

Cryptanalysis of a Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks

Zhenzhen Guo

(Corresponding author: Zhenzhen Guo)

Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China
1550 Haigang Ave, Pudong Xinqu, Shanghai Shi, China
(Email: 925119820@qq.com)

(Received Jan. 8, 2019; revised and accepted Apr. 15, 2019; first on line June 6, 2019)

Abstract

To achieve the secure communication in wireless body area network, various authentication protocols have been proposed. Recently, Ji et al. designed an efficient and certificateless conditional privacy-preserving authentication scheme and claimed that it can realize various security goals like anonymity, mutual authentication, lost PDA attack, replay attack, etc. However, our security analysis shows that the scheme is vulnerable to the modification attack, denial of service attack and impersonation attack.

Keywords: Anonymity; Certificateless; Privacy-preserving; Wireless Body Area Networks

1 Introduction

Wireless body area network(WBAN) is a branch of Wireless Sensor Networks, which can be used to provide telemedicine services to patients. It consists of three entities: sensor nodes, portable personal terminals and application providers. In WBAN, different types of sensors can collect the physiological information of patients in real time, and send the data to application provider through personal terminal, then the application provider analyzes and processes the data accordingly to meet different application requirements [14]. Therefore, it has emerged as a key technology to enhance the quality of life by monitoring and examining the vital signs of patients [4].

Although WBAN has brought us great benefits, it still faces many security challenges. Specifically, because the infrastructures in WBAN have the characteristics of openness, mobility and complexity, it will lead to a malicious attacker launches various attacks such as modification attack, denial of service attack(DoS) and so on. In modification attack, an attacker can distort physiological information of patients, which will lead to the misdiagnosis of doctors and serious medical accidents. In DoS attack, an attacker can send massive service requests to application provider, which will prevent legitimate users from accessing medical services. In addition, the physiological information transmitted in WBAN is important and sensitive for patients. Accordingly, the leakage of privacy is one of the major concerns

of patients [9]. Furthermore, because the sensor nodes in WBAN have stringent resource limitations in energy and storage capacity, the communication protocols for WBAN should be as efficient as possible. Therefore, there are great challenges to realize the security, privacy, reliability of data and the availability of systems [6].

Certificateless public key cryptography solves the key escrow problem existed in Identity-based cryptography [12], which has been widely used in WBAN. Many certificateless authentication schemes [2, 3, 7, 9, 15, 16] have been proposed to realize the secure communication between users and AP in WBAN. Recently, Ji et al. [5] designed an efficient and certificateless conditional privacy-preserving authentication scheme for WBAN. In the scheme, they claimed that it has a unique characteristic, that is, the trusted third parties can extract the real identity of users when necessary. However, our security analysis shows that it failed because it is vulnerable to the modification attack, denial of service attack and impersonation attack.

2 Preliminaries

2.1 Networks Model

Figure 1 demonstrates a typical medical application scenario of WBANs [10]. There are three tiers communications in WBAN: Intra-BAN communications, Inter-BAN communications and beyond-BAN communications [10]. The first layer communications are among sensor nodes and master node, which has more powerful computing and storage capabilities. The second layer communications are between master node and personal device such as PDA, which serves as a gateway for connecting patients to AP. The third layer communications are required to enable an authorized Application Provider to remotely access the medical information of patients via Internet [10]. Correspondingly, the authentication in WBAN is usually divided into three layers: authentication between each pair of sensor nodes, authentication among sensor nodes and PDA, and authentication between PDA and AP [13].

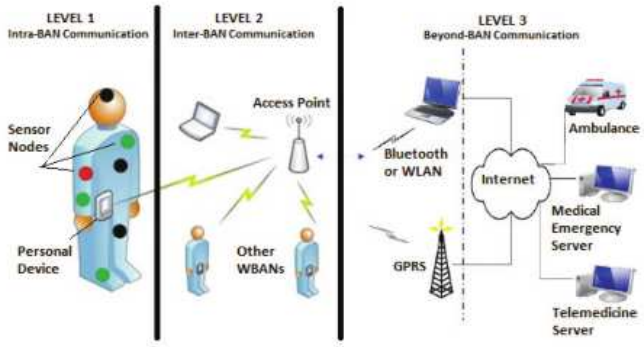

Figure 1: General architecture for Wireless Body Area Networks

Details of the main entities in WBAN are as follows:

Sensor Nodes: The sensor nodes have weak energy and computation ability that can be embedded inside or worn on different parts of human body. They have three main assignments: sensing, processing, and communication. During the sensing, they are able to monitor or perceive various physiological information of patients, such as blood pressure, temperature, Electrocardiography(ECG), Electromyography(EMG) and so on. During the processing, they can perform simple

comparison and storage operations on collected data. During the communication, the processed data can be transmitted to master node for further communication or processing [11].

The gateway between clients and AP: The gateway can be a mobile device carried by user like PDA or smart phone, which is responsible for connecting clients to AP. Because of this property, the gateway subsystem can easily become the weakest link of the overall scenario [1]. In addition, it also need to handle some security issues:

1) Verifying the correct identity of the source,
2) Not modifying the patient data, except for aggregation or other defined transformations,
3) Transmitting the physiological information in time in order that patients can receive timely diagnosis [6].

Application Provider (AP): AP represents the remote medical systems at hospitals or clinics, which is responsible for providing medical services without knowing patients' private information such as name and ID number.

Trusted Authority (TA): TA is a trusted third party who works like a key generation center(KGC). It is in charge of the generation of the system parameters and the registration of clients and AP before communication.

2.2 Security Requirements

Duo to the special structure of WBAN, a malicious attacker can launch various attacks such as modification attack, denial of service attack(DoS) and so on. Therefore, confidentiality and mutual authentication are essential for WBANs, and the transmission must be anonymous and unlinkable as well [8]. Some security requirements of authentication schemes for WBANs are shown in Table 1.

Table 1: security requirements of authentication schemes for WBANs.

Security requirements	Description
Anonymity	Patient's identity must be private and untraceable in the system.
Un-linkability	Adversaries are not able to link two messages sent by the same WBANs client.
Mutual authentication	Senders of patient's data should be able to authenticate with each other.
Session key establishment	The session key between WBANs client and AP should be established.
Attack resistance	The proposed scheme is able to resist various attacks.
Perfect forward security	The previous session keys are still secure even if the long-term private keys of participants are leaked.
Untraceability	Adversaries couldn't trace the action of a specific client through the intercepted messages.
Non-repudiation	The legitimate participants of network can not deny data generated by themselves.

3 Review of Ji et al.'s Scheme

There are four entities in the scheme: WBAN client, AP, TA and PDA. Four phases included in Ji et al.'s scheme.

A. System initialization phase:

TA performs the following:

1) Selects two primes p, q and generates an elliptic curve group G, P is a generator of the group G.
2) Chooses master private key $s \in Z_q^*$ and hash functions: $H_0 : \{0,1\}^* \to z_q^*$, $H_1 : G \to z_q^*$, $H_2 : G \times \{0,1\}^* \to z_q^*$, $H_3 : \{0,1\}^* \times G \times \{0,1\}^* \to z_q^*$.
3) Computes system public key $P_{pub} = sP$.
4) Publishes system parameters $params = \{p, q, F_p, G, P, P_{pub}, H_0, H_1, H_2, H_3\}$.
5) Verifies the real identity ID_A from AP.
6) Selects secret value $z_A \in Z_q$ and computes $b_A = z_A + sH_0(ID_A), B_A = z_A P$ as AP's private key and public key.
7) Sends (b_A, B_A) to AP in a secure channel.

B. Pseudo identity generation and message signing phase:

1) The client performs the following.
   a. Generates two random numbers $r_i, x_i \in Z_p^*$.
   b. Computes partial public key $X_i = x_i P$ and $PID_{i,1} = r_i P$.
   c. Sends real identity RID_i, password PW_i, X_i and $PID_{i,1}$ to TA.
2) Upon receiving $\{RID_i, PW_i, X_i, PID_{i,1}\}$ from the client, TA performs as follows.
   a. Verifies client's real identity RID_i.
   b. Computes $\beta = H_0(RID_i) \oplus H_0(PW_i)$ and $PID_{i,2} = RID_i \oplus H_2(sPID_{i,1}, T)$.
   c. Chooses a secret value $w_i \in Z_p^*$, computes $Y_i = w_i P, y_i = w_i + s \cdot \alpha_i \ mod \ q$, where $\alpha_i = H_1(PID_i, X_i)$ and $PID_i = (PID_{i,1}, PID_{i,2}, T)$.
   d. Loads the pseudo identity PID_i, the partial private key y_i, Y_i and β into PDA.
3) The PDA verifies client's legal identity as follows.
   a. Client inputs the real identity RID_i and password PW_i into PDA.
   b. PDA computes $\beta^* = H_0(RID_i) \oplus H_0(PW_i)$ and verifies $\beta' \stackrel{?}{=} \beta$.
4) PDA generates session key for client as follows.
   a. The client who has passed validation inputs the secret key x_i into PDA.
   b. PDA chooses a secret number $d_i \in Z_p^*$ and computes $D_i = d_i P, \sigma_i = x_i + y_i + d_i \cdot \mu_i \ mod \ q$ and session key $K = d_i(B_A + H_0(ID_A)P_{pub})$, where $\mu_i = H_3(M_i, PID_i, D_i, t_i)$ and M_i is a medical related message.
   c. PDA sends request message$\{PID_i, M_i, \sigma_i, D_i, t_i\}$ to AP, where t_i is time stamp.

C. Authentiation phase:

1) Upon receiving the tuple $\{PID_i, M_i, \sigma_i, D_i, t_i\}$, AP performs as follows.
   a. Checks the freshness of t_i and T in PID_i.
   b. Computes $\alpha_i = H_1(PID_i, X_i)$ and $\mu_i = H_3(M_i, PID_i, D_i, t_i)$.
   c. Checks $\sigma_i P \stackrel{?}{=} X_i + Y_i + \alpha_i \cdot P_{pub} + \mu_i \cdot D_i$. If it holds, AP accepts the request message.
   d. Computes session key $K = b_A D_i$ and message authentication code $MAC_K(B_A)$, sends $MAC_K(B_A)$ to client.
2) Upon receiving the $MAC_K(B_A)$, client performs as follows.

Table 2: authentication and session key generation process in Ji's scheme.

C		PDA		AP
inputs RID_i, PW_i	$\xrightarrow{RID_i, PW_i}$			
		computes:		
		$\beta^* = H_0(RID_i) \oplus H_0(PW_i)$		
		verifies: $\beta' \stackrel{?}{=} \beta$		
inputs x_i	$\xrightarrow{x_i}$			
		chooses: $d_i \in Z_p^*$		
		computes: $D_i = d_i P$		
		$\mu_i = H_3(M_i, PID_i, D_i, t_i)$		
		$\sigma_i = x_i + y_i + d_i \cdot \mu_i \ mod \ q$		
		$K = d_i(B_A + H_0(ID_A)P_{pub})$	$\xrightarrow{PID_i, M_i, \sigma_i, D_i, t_i}$	
				checks: t_i, T
				computes:
				$\alpha_i = H_1(PID_i, X_i)$
				$\mu_i = H_3(M_i, PID_i, D_i, t_i)$
				checks:
				$\sigma_i P \stackrel{?}{=} X_i + Y_i + \alpha_i \cdot P_{pub} + \mu_i \cdot D_i$
				computes:
				$K = b_A D_i$ and $MAC_K(B_A)$
			$\xleftarrow{MAC_K(B_A)}$	
checks $MAC_K(B_A)$				

a. Checks the validity of $MAC_K(B_A)$ by using K. If it holds, client regards K as the session key. The validation equation is as follows:

$$\begin{aligned} \sigma_i P &= (x_i + y_i + d_i \cdot \mu_i) \cdot P \\ &= (x_i + w_i + s \cdot \alpha_i + d_i \cdot \mu_i) \cdot P \\ &= X_i + Y_i + \alpha_i \cdot P_{pub} + \mu_i \cdot D_i \end{aligned}$$

b. The authentication process and session key generation process in Ji et al.'s scheme are shown in Figure 2. Batch authentication of multiple clients is similar to individual authentication of single client. See the original description in [9].

D. Password change phase:

The client inputs the previous password PW_i and the real identity RID_i into PDA. Then PDA Verifies the User's legal identity by computing $\beta' = H_0(RID_i) \oplus H_0(PW_i)$ and verifying $\beta' \stackrel{?}{=} \beta$. The client who has passed validation enters a new password PW_i^*, PDA computes $\beta^* = \beta \oplus H_0(PW_i) \oplus H_0(PW_i^*)$ and replaces β with β^*.

4 Analysis of Ji et al.'s Scheme

Ji et al.'s scheme is an efficient and certificateless conditional privacy-preserving authentication scheme. It satisfies:

Anonymity. The client, who has a real identity and a fixed pseudo-identity, communicates with AP in a pseudo-identity.

Efficient. Ji et al.'s scheme is based on Elliptic Curve Cryptography and big data.

Certificateless. It adopts certificateless encryption system. Due to the certificateless property, PDA only has the partial private key of the WBANs client [5]. The adversary cannot obtain any useful information of patients from the lost PDA.

Conditional. TA can extract the real identity of users when necessary. For one thing, TA can trace the real identity of a malicious client, who cheats AP by sending mendacious messages. For another, when a patient has an emergency, TA can trace this client and help him to get timely treatment [5].

In WBANs, sensor nodes send patient's physiological data to AP for diagnosis through the Personal Digital Assistance(PDA). As mentioned earlier, *PDA can be considered as a gateway between clients and AP, it can easily become the weakest link of the overall scenario* [1]. Therefore, the mutual authentication between users and PDAs is necessary and vital. In Ji's scheme, the equation $\beta' \stackrel{?}{=} \beta$ computed by PDA could only be used to prove the legitimacy of client to PDA. The protocol lacks authentication from PDA to client, it will lead to an illegal PDA mounts various attacks. We describe some attacks launched by an illegal PDA as follows.

Vulnerable to the Dos attack. In Dos attack, network resources will be occupied by substantial service requests launched by attackers, which will lead to legal users unable to access AP's medical services. An illegal PDA chooses many different parameters $\widehat{d_i}, \widehat{t_i}$ and sents massive service requests $\{PID_i, M_i, \widehat{\sigma_i}, \widehat{D_i}, \widehat{t_i}\}$ to AP, where $\widehat{\sigma_i} = x_i + y_i + \widehat{d_i} \cdot \widehat{\mu_i}, \widehat{\mu_i} = H_3((M_i, PID_i, \widehat{D_i}, \widehat{t_i})), \widehat{D_i} = \widehat{d_i}P$. It will pass AP's verification. In fact,

$$\begin{aligned}\widehat{\sigma_i}P &= (x_i + y_i + \widehat{d_i}\widehat{\mu_i})P \\ &= (x_i + w_i + s \cdot \alpha_i + \widehat{d_i}\widehat{\mu_i})P \\ &= X_i + Y_i + \alpha_i \cdot P_{pub} + \widehat{\mu_i}\widehat{D_i}\end{aligned}$$

Vulnerable to the modification attack. Client's service type and rights M_i can be tampered into $\widehat{M_i}$ by an illegal PDA, which will lead to doctor's misdiagnosis and serious medical accidents. An illegal PDA sends the distorted request $\{PID_i, \widehat{M_i}, \widehat{\sigma_i}, D_i, t_i\}$ to AP, which will pass the checking by AP.

$$\begin{aligned}\widehat{\sigma_i}P &= (x_i + y_i + d_i\widehat{\mu_i})P \\ &= (x_i + w_i + s \cdot \alpha_i + d_i\widehat{\mu_i})P \\ &= X_i + Y_i + \alpha_i \cdot P_{pub} + \widehat{\mu_i}D_i\end{aligned}$$

Vulnerable to the impersonation attack. It is noteworthy that the session key between client and AP is generated by PDA in Ji et al.'s scheme, which will lead to key exposure and the impersonation attack launched by illegal PDAs. Firstly, an illegal PDA can communicate with AP and obtain AP's medical service for a long time by utilizing the identity of clients. Similarly, an illegal PDA can obtain users' privacy information by communicating with users as AP.

Through the above analysis, when malicious users deceive AP, TA fails to trace their real identity and punish them. Meanwhile, TA fails to treat patient urgently who has an emergency.

5 Conclusions

In this paper, we reviewed Ji et al.'s certificateless conditional privacy-preserving authentication scheme and pointed out its shortcomings: (1) it lacks the authentication process from PDA to client, (2) the session key between client and AP is known by PDA. Therefore, the scheme can not resist DoS attack, modification attack and impersonation attack. We would like to stressed that the role of PDA cannot be ignored. In order to make the protocol feasible, the structure of WBAN should be clarified before the protocol is proposed.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC 95-2416-H-159-003. We gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey", *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.

[2] R. Guo and H. Shi, "Confidentiality-preserving personal health records in tele-healthcare system using authenticated certificateless encryption," *International Journal of Network Security*, vol. 19, no. 6, pp. 995–1004, 2017.

[3] D. B. He, Z. Sherali, and L. B. Wu, "Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks," *IEEE Systems Journal*, vol. 12, pp. 64–73, 2018.

[4] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu. "Secure anonymous mutual authentication for star two-tier wireless body area networks," *computer methods and programs in biomedicine*, vol. 135, pp. 37–50, 2016.

[5] S. Ji, Z. Gui, T. Zhou, H. Yan, and J. Shen, "An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services," *IEEE Acecess*, vol. 6, pp. 69603–69611, 2018.

[6] W. Leister and H. Abie, "Threat assessment of wireless patient monitoring systems," in *3rd International Conference on Information and Communication Technologies: From Theory to Applications*, 2008.

[7] F. Li, and J. Hong, "Efficient certificateless access control for wireless body area networks," *IEEE Sensors Journal*, vol. 16, no. 13, pp. 5389–5396, 2016.

[8] X. Li, M. H. Ibrahim, and S. Kumari, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, no. 2, pp. 429–443, 2017.

[9] J. Liu, Z. Zhang, X.Chen, X. F, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Transactions on Parallier and Distributed System*, vol. 25, no. 2, pp. 332–342, 2014.

[10] R. Negra, I. Jemili, and A. Belghith, "Wireless Body Area Networks: Applications and Technologies", *Procedia Computer Science*, vol. 83, pp. 1274–1281, 2016.

[11] C. A. Otto, E. Jovanov, and A. Milenkovic, "A WBAN-based System for Health Monitoring at Home," in *3rd IEEE/EMBS International Summer School and Symposium on Medical Devices and Biosensors*, pp. 20–23, 2006.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Advances in Cryptology (CRYPTO'84)*, pp. 47–53, Santa Barbara, California, USA, Aug. 1984.

[13] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems*, vol. 78, no. 3, pp. 956–963, 2018.
[14] J. Shen, Z. Gui, S. Ji, J.Shen, H.Tian, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.
[15] M. Wazid, A. Kumar Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *Journal of Network and Computer Applications*, vol. 123, pp. 112–126, 2018.
[16] F. Wu, L. Xu, S. Kumari, X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multimedia Systems*, vol. 23 , no. 2, pp. 195–205, 2017.

Biography

Zhenzhen Guo is currently pursuing her M.S. degree from Department of Mathematics, Shanghai Maritime university. Her research interests include combinatorics and cryptography.

An Efficient Certificateless Signcryption Scheme without Random Oracles

Shan Shan

(Corresponding author: Shan Shan)

School of Economics and Management, Shandong Jiaotong University
Jinan 250357, China
(Email: jtshanshan@126.com)

(Received Mar. 26, 2019; revised and accepted May 26, 2019; first on line June 6, 2019)

Abstract

Certificateless signcryption is an important multi-function cryptography primitive which solves the key escrow problem in the identity-based cryptosystem and simplifies the certificates management problem in the traditional public key cryptosystem. It simultaneously fulfils the integrated function of public encryption and digital signature with a computing and communication cost significantly smaller than that required by the signature-then-encryption method. In this paper, we propose an efficient certificateless signcryption scheme secure in the standard model. The proposed scheme satisfies the message confidentiality and unforgeability.

Keywords: Certificateless; Signcryption; Standard Model; Random Oracle

1 Introduction

Certificateless public key cryptography (CL-PKC) [1] was introduced by Al-Riyami and Paterson in 2003. Its main idea is that a user's secret including two different parts. One part named secret key is produced by the user himself without requiring the corresponding public key to be certified. Another part named partial private key is generated by a semi-trusted third party, called key generation center (KGC), from the unique identifier information of the user. The user must know both of the secrets to calculate his full private key. CL-PKC is a useful method in solving the certificates management problems, which always accompanied with large amount of computation, storage and communication costs in traditional public key infrastructure and the key escrow problem in identity-based (ID-based) public key cryptography [13].

The confidentiality and authenticity of message is the basic requirement for secure communication. In 1997, Zheng brought the notion of signcryption [16], which simultaneously fulfils the integrated function of public encryption and digital signature with a computing and communication cost significantly smaller than that required by the signature-then-encryption method. As a combining cryptographic primitive, certificateless signcryption (CLSC) scheme was first introduced by Barbosa and Farshim in 2008 [2]. Since then, quite a few schemes related to certificateless or signcryption have been proposed [6–8, 14], but the security of these schemes were proven secure in the random oracle model. Although the model is efficient and useful, it has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure [4]. Therefore, it is an important research problem to construct a CLSC scheme secure in the standard model.

Liu et al. [10] proposed the first CLSC scheme in the standard model and claimed that their scheme satisfies the security requirements of a CLSC scheme. However, their scheme is not even chosen plaintext attack secure by giving a public key replacement attack. Several different attacks were also proposed in the following years [11, 15]. Recently, several CLSC schemes in the standard model have been proposed in [3, 5, 12, 17].

In this paper, we give a new CLSC scheme secure in the standard model. The proposed scheme satisfies the message confidentiality and unforgeability.

The rest of the paper is organized as follows. The complexity assumptions and the formal model of CLSC scheme are introduced in Sect 2. We describe a new concrete CLSC scheme in Sect 3 and give analysis of the new scheme in Sect 4. Finally, the conclusions are given in Sect 5.

2 Preliminaries

2.1 Bilinear Groups

Let G_1, G_2, G_t denote three finite multiplicative abelian groups of large prime order p. Let g be a generator of G_1 and $\tilde{g}$ be a generator of G_2. An admissible asymmetric bilinear pairing is a map $e : G_1 \times G_2 \to G_t$ and satisfies the following properties:

1) $e(g^a, \tilde{g}^b) = e(g, \tilde{g})^{ab}$ for all $a, b \in \mathbb{Z}_p^*$.

2) for $g \neq 1_{G_1}$ and $\tilde{g} \neq 1_{G_2}$, $e(g, \tilde{g}) \neq 1_{G_t}$.

3) e is efficiently computable.

The set $(p, G_1, G_2, G_t, g, \tilde{g}, e)$ is called a bilinear map group system.

2.2 Complexity Assumptions

Here, we present several security assumptions on which our proposed scheme is based.

For a bilinear map group system $(p, G_1, G_2, G_t, g, \tilde{g}, e)$. Choose $(u, v) \in \mathbb{Z}_p$ randomly, a oracle $\mathcal{O}_1(m)$ means that given m, choose a random $r \in \mathbb{Z}_p$ and outputs the tuple $(g^{(u+mv)r}, g^r, \tilde{g}^{\frac{uv}{r}})$. Choose $(x, y, s) \in \mathbb{Z}_p$ randomly, a oracle $\mathcal{O}_2(ID)$ means that given $ID \in \mathbb{Z}_p$, outputs the tuple $(g^{\frac{x}{s+ID}}, g^{\frac{y}{s+ID}}, g^{\frac{1}{s+ID}})$ and a oracle $\mathcal{O}_3(m, ID)$ means that given $(m, ID) \in \mathbb{Z}_p$, choose a random $r \in \mathbb{Z}_p$ and outputs the tuple $(g^{\frac{(x+my)r}{s+ID}}, g^{\frac{r}{s+ID}}, g^r, \tilde{g}^{\frac{y}{r}})$.

Definition 1. *(Modified-PS Assumption 1). Given $g, \tilde{g}, \tilde{g}^u, \tilde{g}^v, g^v$, and unlimited access to the oracle $\mathcal{O}_1$, no adversary can efficiently generate a tuple $(g^{(u+m^*v)r^*}, g^{r^*}, \tilde{g}^{\frac{uv}{r^*}})$, with $g^{r^*} \neq 1_{G_1}$, for a new scalar m^* not asked to $\mathcal{O}_1$.*

Definition 2. *(Assumption 2). Given $g, \tilde{g}, \tilde{g}^s, \tilde{g}^x, \tilde{g}^y, g^x, g^y$ and unlimited access to both oracles $\mathcal{O}_2$ and $\mathcal{O}_3$, no adversary can efficiently generate a tuple $(g^{\frac{(x+m^*y)r^*}{s+ID^*}}, g^{\frac{r^*}{s+ID^*}}, g^{r^*}, \tilde{g}^{\frac{y}{r^*}})$, with $g^{r^*} \neq 1_{G_1}$, for a new scalar ID^* not asked to $\mathcal{O}_2$ and new pair (m^*, ID^*) not asked to $\mathcal{O}_3$.*

For the Modified-PS Assumption 1 and Assumption 2, we refer the reader to [3] for some details.

2.3 Formal Model of CLSC

CLSC scheme consists of following probabilistic polynomial time algorithms.

1) **Setup**

Given a security parameter l, KGC runs this algorithm to generate a master key msk and common parameters $params$. We assume that $params$ are publicly available to all users whereas the msk is kept by the KGC secretly. Formally we can write $(params, msk) \leftarrow Setup(1^l)$.

2) **Extract-partial-private-key**

Given the common parameters $params$, an identity ID, the KGC runs this algorithm to generate the partial private key d associated with ID and transmits it to the user via a secure channel. Formally we can write $d \leftarrow Extract - partial - private - key(params, msk, ID)$.

3) **Set-secret-key**

Given the common parameters $params$ and the identity information ID of himself, each user runs this algorithm to generate a secure value x for himself. Formally we can write $x \leftarrow Set - secret - Key(params, ID)$.

4) **Set-private-key**

Given the common parameters $params$, the partial private key d and the secret value x, the user with identity ID runs this algorithm to generate the full private key SK for himself. Formally we can write $SK \leftarrow Set - private - key(params, x, d)$.

5) **Set-public-key**

Given the common parameters $params$, the partial private key d, the secret value x, the user with identity ID runs this algorithm to generate the full public key PK as the output. Formally we can write $PK \leftarrow Set - public - key(params, x, d)$.

6) **CLSC-signcrypt**

Given the common parameters $params$, the message m, the receiver's identity ID_B and the full public value PK_B, the user with identity ID_A and the full private key SK_A runs this algorithm to generate the ciphertext δ as the output. Formally we can write $(ID_A, ID_B, \delta) \leftarrow CLSC - signcrypt(params, m, ID_A, SK_A, ID_B, PK_B)$.

7) **CLSC-unsigncrypt**

Given the ciphertext δ, the sender's identity ID_A and the public key PK_A, the receiver with identity ID_B and the full private key SK_B runs this algorithm to unsigncrypt the ciphertext and returns m or $\perp$. Formally we can write $(m/\perp) \leftarrow CLSC-unsigncrypt(params, \delta, ID_A, PK_A, ID_B, SK_B)$.

For consistency, we require that if $(ID_A, ID_B, \delta) \leftarrow CLSC-signcrypt(params, m, ID_A, SK_A, ID_B, PK_B)$, then the output of $CLSC - unsigncrypt(params, \delta, ID_A, PK_A, ID_B, SK_B)$ must be m.

3 The Concrete Scheme

In this section, based on Canard et al.'s signature scheme [3], we present a novel CLSC scheme:

1) **Setup**

The KGC generates the system parameters $params$ and a master key msk, given a security parameters $l \in \mathbb{Z}^+$ as input, the KGC executes the following operations:

- Chooses a l-bits prime p and generates a bilinear map group system $(p, G_1, G_2, G_t, g, \tilde{g}, e)$.

- Let H be a cryptography hash function where $H : G_t \to \mathbb{Z}_p$
- Chooses $(s, x, y) \in \mathbb{Z}_p^*$ randomly.
- The public parameters are presented as $Params = (g, \tilde{g}, \tilde{S} = \tilde{g}^s, \tilde{X} = \tilde{g}^x, \tilde{Y} = \tilde{g}^y, X = g^x, Y = g^y)$, and the master key is $msk = (s, x, y)$.

2) **Extract-partial-private-key**

The user **U** sends $ID_u \in \mathbb{Z}_p^*$ to the KGC. In turn, the KGC generates and returns the partial private key of **U** as $d_u = (d_{1,u}, d_{2,u}, d_{3,u}) = (g^{\frac{x}{s+ID_u}}, g^{\frac{y}{s+ID_u}}, g^{\frac{1}{s+ID_u}})$.

3) **Set-secret-key**

The user **U** with the identity ID_u randomly chooses $x_u \in \mathbb{Z}_p^*$ as its secret key.

4) **Set-private-key**

The user **U** takes the pair (x_u, d_u) as its full private key SK_u.

5) **Set-public-Key**

The user **U** takes $PK_u = \tilde{g}^{x_u}$ as its public key.

6) **CLSC-signcrypt**

With ID_B as the receiver and the message $m \in G_t$, the sender **A** performs as follows:

- Chooses $(r_1, r_2) \in \mathbb{Z}_p^*$ randomly.
- Computes $U = (d_{1,A})^{r_1} \cdot (d_{2,A})^{H(m)r_1} \cdot (d_{3,A})^{x_A r_1} = g^{\frac{(x+x_A+H(m)y)r_1}{s+ID_A}}$.
- Computes $N = g^{r_1}$,$V = (d_{3,A})^{r_1}$ and $L = \tilde{Y}^{\frac{x_A}{r_1}} = \tilde{g}^{\frac{x_A y}{r_1}}$.
- Computes $c = m \cdot e(g, PK_B)^{-r_2}$ and $Z = \tilde{S}^{r_2}\tilde{g}^{r_2 ID_B} = \tilde{g}^{r_2(s+ID_B)}$.
- Sets $\delta = (U, N, V, L, c, Z)$ and return (ID_A, ID_B, δ) as the ciphertext.

7) **CLSC-unsigncrypt**

Given the ciphertext $(ID_A, ID_B, \delta = (U, N, V, L, c, Z))$, the receiver **B** decrypts and verifies the ciphertext as follows:

- Computes $m' = c \cdot e(d_{3,B}, Z)^{x_B}$.
- Computes $U' = \tilde{S}\tilde{g}^{ID_A}$ and $W = \tilde{X} \cdot PK_A \cdot \tilde{Y}^{H(m)} \cdot \tilde{g}$.
- Checks if $e(U \cdot V, U')e(N, L) = e(N, W) \cdot e(Y, PK_A)$. If the equation not holds, then return $\perp$ indicating the message is not valid. Otherwise, return m' indicating it is a valid signcryption ciphertext of the message m sending to receiver **B**.

4 Analysis of the Proposed Scheme

4.1 Correctness

We proceed to prove that our proposed concrete scheme is consistent and correct.

$$\begin{aligned} m' &= c \cdot e(d_{3,B}, Z)^{x_B} \\ &= m \cdot e(g, PK_B)^{-r_2} \cdot e(g^{\frac{1}{s+ID_B}}, \tilde{S}^{r_2} \tilde{g}^{r_2 ID_B})^{x_B} \\ &= m \cdot e(g, \tilde{g}^{x_B})^{-r_2} \cdot e(g^{\frac{1}{s+ID_B}}, \tilde{g}^{r_2(s+ID_B)})^{x_B} \\ &= m \cdot e(g, \tilde{g})^{-r_2 \cdot x_B} \cdot e(g, \tilde{g})^{r_2 \cdot x_B} \\ &= m \end{aligned}$$

$$\begin{aligned} e(U \cdot V, U')e(N, L) &= e(U \cdot V, U')e(N, L) \\ &= e(g^{\frac{(x+x_A+H(m)y)r_1}{s+ID_A}} \cdot (d_{3,A})^{r_1}, \tilde{S}\tilde{g}^{ID_A})e(g^{r_1}, \tilde{g}^{\frac{x_A y}{r_1}}) \\ &= e(g^{\frac{r_1(x+x_A+H(m)y+1)}{s+ID_A}}, \tilde{g}^{s+ID_A})e(g^{r_1}, \tilde{g}^{\frac{x_A y}{r_1}}) \\ &= e(g^{r_1}, \tilde{g}^{(x+x_A+H(m)y+1)})e(g^y, \tilde{g}^{x_A}) \\ &= e(N, W)e(Y, PK_A) \end{aligned}$$

4.2 Security

4.2.1 Confidentiality

Theorem 1. *The new CLSC scheme is indistinguishability against adaptive chosen ciphertext attacks launched by Type I and Type II attacker respectively.*

4.2.2 Unforgeability

Theorem 2. *The new CLSC scheme is existential unforgeability against adaptive chosen message attacks launched by Type I and Type II forger respectively.*

4.3 Performance Analysis

We compare our scheme with several existing schemes from two aspects: CLSC-signcrypt and CLSC-unsigncrypt and pay attention to those operations such as a bilinear pairing operation, pairing-based exponentiation operation and scalar multiplication operation. We define the notations in Table 1, and adopt the experiment testing results from [9].

The comparison is shown in Tables 2, $|G_1|$ denote the size of an element in G_1, $|G_2|$ denotes the size of an element in G_2 used in the existing schemes or G_t used in the new scheme.

From Table 2, it shows that the new CLSC scheme needs much less computational time than the other schemes.

5 Conclusion

Certificateless signcryption can provide message confidentiality and unforgeability in the absence of a trusted third party. In this paper, we propose a new CLSC scheme secure in the standard model.

Table 1: Notation and definition of diffident time complexities

Notations	**Definition and conversion**
T_{Mul}	Time required for executing a modular multiplication operation
T_E	Time required for executing a pairing-based exponentiation $T_E \approx 43.5\,T_{Mul}$
T_M	Time required for executing a elliptic curve scalar point multiplication $T_M \approx 29\,T_{Mul}$
T_P	Time required for executing a bilinear pairing operation $T_P \approx 87\,T_{Mul}$

Table 2: Comparisons of the computational overhead and storage costs

Schemes	**Ciphertext size**	**CLGSC-signcrypt time**	**CLGSC-unsigncrypt time**
Cheng et al. [5]	$4\|G_1\| + \|G_2\|$	$(5T_P + 3T_M + T_E) \approx 565.5\,T_{Mul}$	$10T_P \approx 870\,T_{Mul}$
Zhou et al. [17]	$4\|G_1\| + 2\|G_2\|$	$(2T_P + 5T_M + 3T_E) \approx 449.5\,T_{Mul}$	$(7T_P + 2T_M) \approx 667\,T_{Mul}$
Rastegari et al. [12]	$4\|G_1\| + \|G_2\|$	$(2T_P + 7T_M) \approx 377\,T_{Mul}$	$(7T_P + T_M) \approx 638\,T_{Mul}$
Proposed	$5\|G_1\| + \|G_2\|$	$(T_P + 8T_M + T_E) \approx 362.5\,T_{Mul}$	$(5T_P + 2T_M + T_E) \approx 536.5\,T_{Mul}$

According to the comparison with other schemes in the same model, the new scheme is efficient and practical.

References

[1] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of Cryptology-ASIACRYPT 2003,Lecture Notes in Computer Science 2894*, pp. 452–474, Taipei, China, November 2003.

[2] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS 2008)*, pp. 369–372, Tokyo, Japan, March 2008.

[3] S. Canard and V. C. Trinh, "An efficient certificateless signature scheme in the standard model," in *Proceedings of ICISS16, Lecture Notes in Computer Science 10063*, pp. 175–192, Jaipur, India, December 2016.

[4] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology," *Journal of the ACM*, vol. 51, no. 4, pp. 557–594, 2004.

[5] L. Cheng and Q. Y. Wen, "An improved certificateless signcryption in the standard model," *International Journal of Network Security*, vol. 17, no. 5, pp. 597–606, 2015.

[6] G. M. Gao, X. G. Peng, and L. Z. Jin, "Efficient access control scheme with certificateless signcryption for wireless body area networks," *International Journal of Network Security*, vol. 21, no. 3, pp. 428–437, 2019.

[7] R. Guo and H. X. Shi, "An efficient confidentiality preserving scheme using certificateless encryption with high trust level," *International Journal of Network Security*, vol. 20, no. 1, pp. 78–87, 2018.

[8] D. B. He, M. K. Khan, and S. H. Wu, "On the security of a rsa-based certificateless signature scheme," *International Journal of Network Security*, vol. 16, no. 1, pp. 78–80, 2014.

[9] S. Islam and G. Biswas, "Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography," *International Journal of Computer Mathematics*, vol. 90, no. 11, pp. 2244–2258, 2013.

[10] Z. Liu, X. Zhang Y. Hu, and H. Ma, "Certificateless signcryption scheme in the standard model," *Information Science*, vol. 180, no. 3, pp. 452–464, 2010.
[11] S. Q. Miao, F. T. Zhang, S. J. Li, and Y. Mu, "On security of a certificateless signcryption scheme," *Information Science*, vol. 232, pp. 475–481, 2013.
[12] P. Rastegari and M. Berenjkoub, "An efficient certificateless signcryption scheme in the standard model," *International Journal of Information Security*, vol. 9, no. 1, pp. 3–16, 2017.
[13] A. Shamir, "Identity-based cryptosystem and signature scheme," in *Proceedings of Cryptology-CRYPTO 1984, Lecture Notes in Computer Science 196*, pp. 120–126, Santa Barbara, California, USA, August 1984.
[14] G. Sharma, S. Bala, and A. K. Verma, "An improved rsa-based certificateless signature scheme for wireless sensor networks," *International Journal of Network Security*, vol. 18, no. 1, pp. 82–89, 2016.
[15] J. Weng, G. X. Yao, R. H. Deng, M. R. Chen, and X. X. Li, "Cryptanalysis of a certificateless signcryption scheme in the standard model," *Information Science*, vol. 181, no. 3, pp. 661–667, 2011.
[16] Y. L. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost (encryption)," in *Proceedings of Cryptology-CRYPTO 1997, Lecture Notes in Computer Science 1294*, pp. 165–179, Santa Barbara, California, USA, August 1997.
[17] C. X. Zhou, G. Y. Gao, and Z. M. Cui, "Certificateless signcryption in the standard model," *Wireless Personal Communications*, vol. 92, no. 2, pp. 495–513, 2017.

Biography

Shan Shan is currently a lecturer in the School of Economics and Management in Shandong Jiaotong University, China. Her research interests include electric commerce and information security.

Review on Nuida-Kurosawa Fully Homomorphic Encryption in Client-server Computing Scenario

Yang Li

(Corresponding author: Yang Li)

Department of Mathematics, Shanghai Maritime University
Haigang Ave 1550, Shanghai, 201306, China
(Email: 553183984@qq.com)

(Received Apr. 19, 2019; Revised and Accepted June 26, 2019; First Online July 18, 2019)

Abstract

Fully homomorphic encryption (FHE) is a common cryptographic primitive that allows anyone to calculate encrypted data without the decryption key. It is especially important for confidential information security and privacy protection. In this paper, we review the Nuida-Kurosawa FHE scheme in the context of mathematics and find some flaws. By adding a key filtering process and applying it to the client-server computing scenario. At the same time, we want to emphasize that modular operation is the fundamental way to dissipate and obscure redundancies in plaintext. Finally, we propose a model extension of the scheme.

Keywords: Client-server; Computing Scenario; Fully Homomorphic Encryption; Magnification Method; Modular Arithmetic; Symmetric Secret Key

1 Introduction

The word homomorphism is derived from the Greek word homos meaning "same" and morphe meaning "shape", which is a mapping of mathematical algebraic system convert into or onto another algebraic system or itself. In cryptography, homomorphic encryption is used in conversion of plaintext and ciphertext operations. It is an effective cryptography method that protects security of privacy and data. Homomorphic encryption (HE) introduced by Rivest, Adleman and Dertouzos [26] in 1978, is a useful cryptographic tool because it can allow one to perform arbitrary arithmetic operation on ciphertext without the decryption key. This particular property can be applied in many fields, such as cloud computing, private queries, the Internet of Things, electronic voting, spam filtering, and more. For example, a user wants to make a private query on search engines. The encrypted query request is sent to the search engine, which can calculate it and return the result to the user, who decrypts it to get the desired result. When authorized user wants to obtain the plaintext result, he only needs to decrypt received ciphertext with the authorized decryption key. This computing process averts frequent encryption and decryption operations under the traditional encryption. Throughout the process, sensitive data are always stored in an encrypted form and only one interaction of data is required. The cloud server can perform arbitrarily computations on encrypted data without decryption key.

The powerful homomorphic encryption scheme supports either addition or multiplication operations (but not both) on encrypted data and translates corresponding plaintext operations into ciphertext. In 2009, Gentry [12] proposed a somewhat homomorphic encryption scheme based on the ideal lattice, which was improved into FHE scheme by adding conditions and bootstrapping method in his PhD dissertation. The Gentry's scheme is the first FHE scheme which makes it possible to evaluate some functions in the encrypted domain. However, the limitation of computational complexity hinders it to apply in practice. Since then, FHE technology has entered a period of rapid development. Many scholars were inspired by Gentry and have proposed a series of FHE schemes based on bit, integer and polynomial rings. Van Dijk [10] constructed an elementary modular arithmetic FHE scheme for handling integers instead of bits, which is more efficient than previous schemes. At Eurocrypt' 10, Gentry, Halevi and Vaikuntanathan [14] proposed a FHE scheme based on Learning With Error (LWE) problem. Coron *et al.* [7] constructed a FHE scheme based on ring-LWE over integers to reduce the public key size, which was improved by Stehle and Steinfeld [27]. In the article *Homomorphic Encryption Can be Applied to the Actual*? , Lauter [18] focused on the calculation operation on encrypted data. The computations used may calculate averages, standard deviations and logical expressions which can be used to predict some healthy problems in life. In 2011, Gentry and Halevi [13] improved a previous scheme on the ideal lattices, but calculation is still complicated and inefficient. In 2013, Monique Ogburn *et al.* [24] discussed the concepts and significance of homomorphic encryption along with subdivisions and limitations associated with this type of encryption scheme. Gupta and Sharma [15] proposed a FHE scheme using a symmetric key of a smaller size, involving operations such as the matrix inversion and the matrix calculation, thus the calculation cost is slightly higher.

With the development of the Internet, cloud computing is deemed as the one of the most powerful innovations in the field of information technology. Many types of encryption algorithms are used for protecting data. The FHE scheme makes it possible to operate on encrypted data, which is different from the traditional encryption method. The existing schemes [3, 4, 21, 29] are still too inefficient, computing complex and hardly applied in practice. In 2014, Nitesh Aggarwal *et al.* [2] stated a symmetric FHE scheme and had performance superior to existing public-key schemes. Potey *et al.* [25] presented an efficient and practical homomorphic encryption scheme which performed on low-size encrypted data on AWS. In 2017, Song *et al.* [28] proposed a hybrid cloud computing scheme based on the Paillier and RSA algorithm. Kim and Tibouchi [16] proposed a new fully homomorphic encryption over the integers and modular arithmetic circuits, compared with van Dijk scheme and Nuida-Kurosawa [23] FHE scheme and showed which is preferable. A variant of FHE, for Q-ary plaintexts where $Q > 2$ is a prime, was subject to Refs. [6, 19]. The works [1, 9] discussed FHE scheme over polynomial rings. Researchers all over the world are concerned about developing homomorphisms that can be used in cloud computing or other fields [8, 11, 17, 20, 22, 28]. Cao *et al.* [5] stressed that cryptography uses modular arithmetic a lot in order to obscure and dissipate redundancies in plaintext, not to preform any numerical calculations.

Recently, we find that some FHE schemes have drawbacks due to the neglect of certain conditions. We would stress that modular arithmetic is used to confuse and diffuse plaintext against statistical attacks. Although the Nuida-Kurosawa FHE scheme is safe, there are drawbacks in special computing situations. This article focuses on the application of the client-server scenario and analyzes the causes of its defects. Many researchers ignore the differences between algebra and polynomial in modular operations and cause computational errors in some special cases. This paper mainly studies that random key needs to be in a certain interval. At the same time, a special example will be used for analysing in the paper. If appropriate random number is selected as private key, the Nuida-Kurosawa FHE scheme is correct in all cases. In this paper, we analyze the reason and improve the interval of key selection process of the Nuida-Kurosawa FHE scheme to implement the FHE scheme without changing the security.

The rest of this paper is organized as follows. Section 2 describes the definitions of modular arithmetic

and homomorphism. In Section 3, we revisit the Nuida-Kurosawa FHE scheme and calculate an example of a client-server computing scenario. In Section 4, we analyze the existing shortcomings, describe our main ideas, algorithms and models, and calculate an example on the modified scheme. We establish a generalized model in Part 5. Finally, the conclusions are given in Section 6.

2 Mathematic Background and Modular Arithmetic

A common Equation which includes variables, constants and operators. There are three kinds of expressions: arithmetic expression, logical expressions and relational expression. Arithmetic operators include addition $(+)$, substraction $(-)$, multiplication $(\cdot)$, modular (mod) and so on.

In mathematics, homomorphism is a mapping from a set into or onto another set or itself.

$$v = f(u) \Leftrightarrow Enc(v) = g(Enc(u))$$

where v and u belong to plaintext domain (the first set). f and g are related functions. $Enc()$ is the encrypted operation on elements in the first set.

For $a, b \in \mathbb{Z}_p$ where p is a prime, $E()$ is a homomorphic encryption operation and $D()$ is a corresponding homomorphic decryption operation. Homomorphism has the following properties.

$$\begin{aligned} D(E(a) + E(b)) &= D(E(a+b)) = a + b \mod p \\ D(E(a) \cdot E(b)) &= D(E(ab)) = ab \mod p. \end{aligned}$$

Specially,

$$a + b \mod p \mod q \nRightarrow a + b \mod q \mod p$$
$$ab \neq (ab \mod p), \quad a + b \neq (a + b \mod p).$$

Here, we want to stress that p and q need reasonable selection. Modular arithmetic can obscure the relationship between the plaintext and ciphertext and reduce computing cost. To illustrate this point, we will carefully study the symmetric version of FHE scheme proposed by Nuida and Kurosawa.

3 Nuida-Kurosawa FHE Scheme

3.1 Description

In 2010, Dijk *et al.* proposed a FHE scheme based on integers. The plaintext space is $\mathcal{M} = \mathbb{Z}_2$ and the ciphertext c of a plaintext $m \in \mathcal{M}$ is $c = pq + 2r + m$, where p is a secret prime and r is a small noise. In their scheme, the decryption is given by $m = (c \mod p) \mod 2 = c - p \cdot \lfloor c/p \rceil \mod 2$. This scheme encrypts each bit and is complex because it has to generate some bits to hide one bit. In 2015, Nuida and Kurosawa proposed a FHE scheme over the integers with message space $\mathbb{Z}_Q$ where Q is a prime. The degree of the decryption circuit is smaller than the previous scheme and the scheme is more efficient. Obviously, this is a conversion of Boolean circuit and arithmetic circuit. We mainly study symmetric version of Nuida-Kurosawa FHE scheme and describe it as follows.

Keygen(λ): For a security parameter λ, select an odd number $p \in [2^{\lambda-1}, 2^{\lambda})$ and set it as the secret key.

Encrypt(p, m): Given a message $m \in \mathbb{Z}_Q$, calculate the ciphertext as

$$c = pq + Qr + m,$$

where the integers q, r are chosen at random in some other prescribed intervals, such that $Qr < |p/2|$.

Decrypt(p, c)**:** $m = (c \mod p) \mod Q$.

Additive homomorphic property: $(c_1 + c_2) \mod p \mod Q = m_1 + m_2$.

Multiplicative homomorphic property: $(c_1 \cdot c_2) \mod p \mod Q = m_1 \cdot m_2$.

3.2 An Example

The user has two numbers $m_1 = 5$, $m_2 = 1$ and wants a server to help him to calculate $f(m_1, m_2) = m_1 + m_2$. Suppose that user selects $p = 7919$ as secret key. First, he selects Q, r and q according to above require in the FHE scheme. Second, he encrypts m_1 and m_2 and obtains corresponding ciphertexts c_1 and c_2. Third, he sends c_1 and c_2 to the server. The server computes $c_1 + c_2$ with function $f(x, y) = x + y$. Finally, server sends obtained result to user. Table 1 describes this process.

Table 1: Nuida-Kurosawa FHE symmetric scheme

Input	Function: $f(x, y) = x + y$
$Q = 3$, $r_1 = 57$, $r_2 = 85$, $p = 7919$, $q_1 = 1325$, $q_2 = 5538$, $m_1 = 5$, $m_2 = 1$	$f(m_1, m_2) = m_1 + m_2$
Encrypt: $c_1 = pq_1 + Qr_1 + m_1 = 7919 \cdot 1325 + 3 \cdot 57 + 5 = 10492851$ $c_2 = pq_2 + Qr_2 + m_2 = 7919 \cdot 5538 + 3 \cdot 85 + 1 = 43855678$	Ciphertext sum: $c_1 + c_2$=54348529
Decrypt: $(c_1 + c_2) \mod p \mod Q = 54348529 \mod 7919 \mod 3$	Decryption result: $0 \neq 5 + 1$

3.3 Wrong Out and Analysis

In [5], Cao *et al.* emphasized that the carry problem can't be handled in the client-server scenario for the van Dijk scheme. Nuida-Kurosawa FHE scheme is improved by defining $Qr < |p/2|$. However, the server can't return the correct value for the simple function $f(x, y) = x + y$.

The above FHE scheme exists drawbacks for two reasons: One is that the author can't choose a secret key in the appropriate interval; another reason is that the difference between algebra and polynomial in modular operation is ignored. We will verify the multiplicative homomorphism in a mathematical context as follows.

$$\begin{aligned}
&(pq_1 + Qr_1 + m_1) \cdot (pq_2 + Qr_2 + m_2) \bmod p \bmod Q \\
&= p^2 q_1 q_2 + pQq_1 r_2 + pq_1 m_2 + Qr_1 pq_2 + Q^2 r_1 r_2 + Qr_1 m_2 + m_1 pq_2 + m_1 Qr_2 + m_1 m_2 \bmod p \bmod Q \\
&= [p(pq_1 q_2 + Qq_1 r_2 + q_1 m_2 + Qr_1 q_2 + m_1 q_2) + Q(Qr_1 r_2 + r_1 m_2 + m_1 r_2) + m_1 m_2] \bmod p \bmod Q \\
&= Q(Qr_1 r_2 + r_1 m_2 + m_1 r_2) + m_1 m_2 \bmod Q \\
&= m_1 m_2.
\end{aligned} \tag{1}$$

In Equation (1), if $Q(Qr_1 r_2 + r_1 m_2 + m_1 r_2) > p$, the result will be unequal to $m_1 m_2$. In Equation (2), we find that the process is flawed. We may sometimes neglect the difference between algebraic and

polynomial in modular operations.

$$\begin{aligned}&[p(pq_1q_2 + Qq_1r_2 + q_1m_2 + Qr_1q_2 + m_1q_2) + Q(Qr_1r_2 + r_1m_2 + m_1r_2) + m_1m_2] \bmod p \bmod Q \\ &= Q(Qr_1r_2 + r_1m_2 + m_1r_2) + m_1m_2 \bmod Q \\ &= m_1m_2.\end{aligned} \tag{2}$$

How to deal with this error? We will filter the generated keys and choose the key in the appropriate interval. In the next section, we will provide some improvements to make the scheme more complete.

4 The Proposal Scheme

4.1 Main Idea

For the problem mentioned above, one way to solve the defects is to select the key in the appropriate interval to ensure correctness. Modular operation is the useful method for reducing computational cost and obfuscating ciphertext in the field of information security. If the chosen parameters aren't suitable, the modular arithmetic might be of little importance for the FHE scheme. On the other hand, we can convert it to other circuits (rings, finite fields and so on) and construct a homomorphic scheme by numerical calculation. Here, we apply the first method: choose the key in a fixed interval.

4.2 The Revised Scheme

The Algorithm. 1 describes this scheme as follow.

Algorithm 1 Pick key

1: pick secret key $p \in [2^{\lambda-1}, 2^{\lambda}]$, an odd number, (Q is published).
2: random select r, q, r is a small number ($r \ll p$), such that $Qr < |p/2|$.
3: **while** $p \notin [\lceil Q^2(max\{r_1, r_2\})^2 + Q^2(max\{r_1, r_2\}) + \frac{Q^2}{4}\rceil, +\infty]$ **do**
4: select random secret key p again.
5: **end while**
6: compute Additive homomorphic and Multiplicative homomorphic
7: End

KeyGen(λ): Generate a random p and set it as the secret key.

Key Judgement(p, Q, r)**:** Q is published, the integers q, r are chosen at random in some other prescribed intervals, such that $Qr < |p/2|$. If satisfy Equation (3), set it as the secret key, otherwise generate secret key again.

$$p \in [\lceil Q^2(max\{r_1, r_2\})^2 + Q^2(max\{r_1, r_2\}) + \frac{Q^2}{4}\rceil, +\infty] \tag{3}$$

Encrypt(p, m)**:** Given a bit $m \in \mathbb{Z}_Q$, calculate the ciphertext as

$$c = pq + Qr + m$$

where the integers q, r are chosen at random in some other prescribed intervals, such that $Qr < |p/2|$.

Decrypt(p, c)**:** $m = (c \mod p) \mod Q$.

Additive homomorphic property: $(c_1 + c_2) \mod p \mod Q = m_1 + m_2$.

Multiplicative homomorphic property: $(c_1 \cdot c_2) \mod p \mod Q = m_1 \cdot m_2$.

The interval of key generation is determined by the method of amplification as follows.

$$\begin{aligned} Q(Qr_1r_2 + r_1m_2 + m_1r_2) + m_1m_2 &< Q^2(max\{r_1, r_2\})^2 + 2Q(max\{r_1, r_2\})max\{m_1, m_2\} + \frac{Q^2}{4} \\ &< Q^2(max\{r_1, r_2\})^2 + Q^2(max\{r_1, r_2\}) + \frac{Q^2}{4} < p \end{aligned} \tag{4}$$

The key selection process is shown in Figure 1.

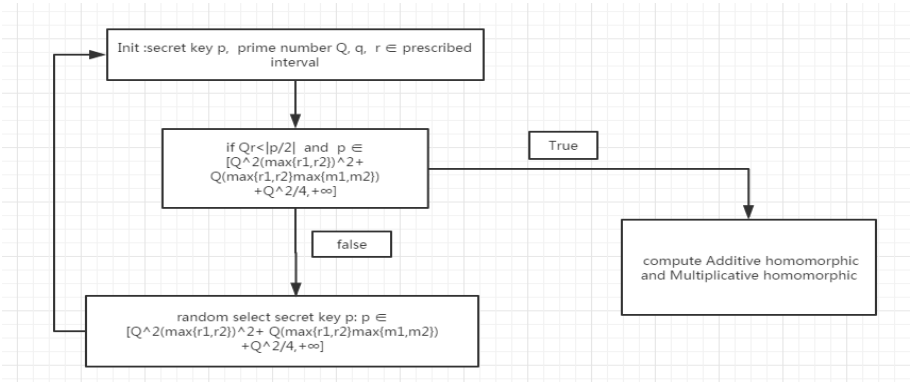

Figure 1: Key selection process

4.3 An Example

For $m_1 = 5$, $m_2 = 1$, server computes function $f(m_1, m_2) = m_1 + m_2$. Given $m \in \mathbb{Z}_Q$, Q is any prime. Suppose that one client sets $Q = 11$, $r_1 = 57$, $r_2 = 85$, $q_1 = 1325$, $q_2 = 5538$. By Equation (3), the secret key interval is $p \in [\lceil 884540.25 \rceil, +\infty]$. If the original generated session key doesn't belong to this interval, client requests it again until it belongs to this interval. So randomly choose session key $p = 884543$.

$$c_1 = pq_1 + Qr_1 + m_1 = 884543 \cdot 1325 + 11 \cdot 57 + 5 = 1172020107.$$

$$c_2 = pq_2 + Qr_2 + m_2 = 884543 \cdot 5538 + 11 \cdot 85 + 1 = 4898600070.$$

Additive homomorphic:

$$c_1 + c_2 \mod p \mod Q = 6070620177 \mod 883678 \mod 11 = 6.$$

Multiplicative homomorphic:

$$c_1 \cdot c_2 \mod p \mod Q = 5741257778191607490 \mod 883678 \mod 11 = 5.$$

5 New Model

For $i = 1, \ldots, n$, let $m_i \in \mathbb{Z}_Q$. When we want to compute $m_1 + m_2 + \ldots + m_n$ using FHE scheme, we can rely on this model which describes in following Figure 2.

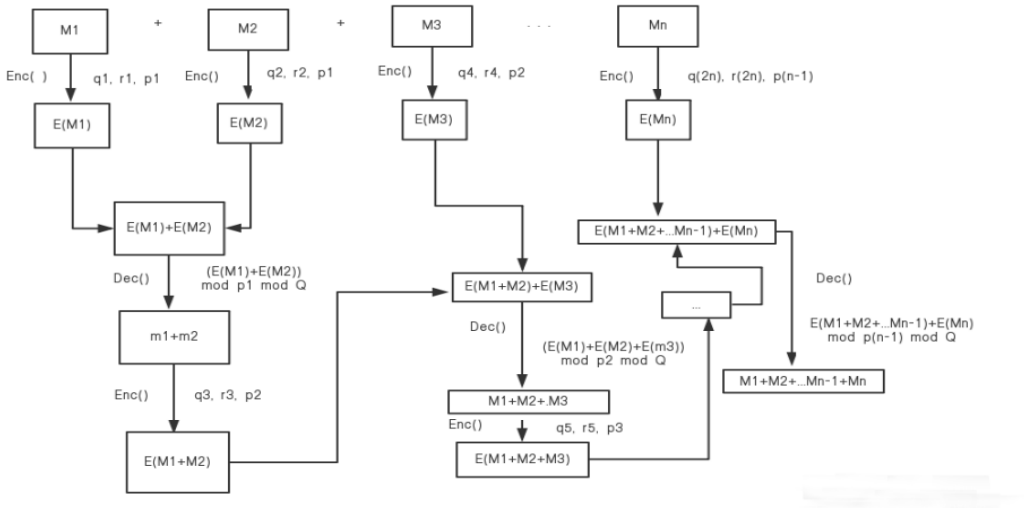

Figure 2: The New Scheme

We generalize this scheme for n inputs in client-server computing scenario. For example, a client wants to compute $m_1 + m_2 + \ldots + m_n$. All $p_1, \ldots, p_{n-1}$ are selected according to Algorithm 1. Q is published. The client encrypts $m_1, m_2 \in \mathbb{Z}_Q$ and chooses q_1, q_2, r_1, r_2, p_1 according to above revised theme, sends c_1, c_2 to the server. Then the server computes $m_1 + m_2$ by converting into corresponding $c_1 + c_2$ with q_1, q_2, r_1, r_2, p_1 and client decrypts $c_1 + c_2$ as $m_1 + m_2$. Next, encrypt $m_1 + m_2, m_3 \in \mathbb{Z}_Q$ separately with q_3, q_4, r_3, r_4, p_2, and computes $c_1 + c_2 + c_3, \ldots, +c_n$. Finally, client obtains result of $m_1 + m_2 + \ldots + m_n$.

6 Conclusion

We want to emphasize how to determine the value range of the session key and analyze the cause of the error. There are two reasons for the error: the interval of the key is not determined, the difference between the polynomial and the algebra for the modular arithmetic is neglected. Choosing a random key in the correct domain is a basic operation. In this paper, we perform FHE scheme with the appropriate key in the client-server scenario. We solve the previous error situation and get the correct result. Finally, the symmetric version of Nuida-Kurosawa FHE scheme has been improved. In the future, we will apply it to other scenarios and study the asymmetrical version of Nuida-Kurosawa FHE scheme.

References

[1] K. Aganya, I. Sharma, "Symmetric fully homomorphic encryption scheme with polynomials operations," in *Proceedings of the 2nd International conference on Elctronics, Communication and*

Aerospace Technology (ICECA'18), pp. 1954-1957, 2018.

[2] N. Aggarwal, C. P. Gupta, I. Sharma, "Fully homomorphic symmetric scheme without bootstrapping," in *International Conference on Cloud Computing and Internet of Things (CCIOT'14)*, 2014.

[3] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) Fully homomorphic encryption without bootstrapping," in *Proceedings of ACM Conference on Innovations in Theoretical Computer Science (ITCS'12)*, Cambridge, MA, USA, Jan. pp. 309-325, 2012.

[4] Z. J. Cao and L. H. Liu, "Comment on harnessing the cloud for securely outsourcing large-scale systems of linear equations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 5, pp. 1551-1552, 2016.

[5] Z. J. Cao, L. H. Liu and Y. Li, "Ruminations on fully homomorphic encryption in client-server computing scenario," *International Journal of Electronics and Information Engineering*, Vol. 8, No1, pp. 32-39, Mar. 2018.

[6] H. J. Cheon, K. Han and D. Kim, "Faster bootstrapping of FHE over the integers," *IACR Cryptology ePrint Archive*, vol. 79, 2017. (`http://eprint.iacr.org/2017/079`)

[7] J. S. Coron, A. Mandal, D. Naccache, M. Tibouchi, "Fully homomorphic encryption over the integers with shorter public-keys," in *Advances in Cryptology-CRYPTO'11*, Springer, Berlin, Heidelberg, pp. 487-504, 2011.

[8] D. Das, "Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation," in *ICOIN'18*, pp. 391-396, 2018.

[9] S. Dasgupta, S. K. Pal, "Design of a polynomial ring based symmetric homomorphic encryption scheme," *Perspectives in Science*, pp. 692-695, 2016.

[10] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *in Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'10)*, pp. 24-43, 2010.

[11] A. El-Yahyaoui and M. D. Ech-Cherif El Kettani, "An efficient fully homomorphic encryption scheme," *International Journal of Network Security*, vol. 21, no. 1, pp. 91-99, Jan. 2019.

[12] C. Gentry, "A fully homomorphic encryption using ideal lattices," in *STOC*, vol. 9, pp. 169-178, 2009.

[13] C. Gentry and S. Halevi, "Implementing Gentrys fully homomorphic encryption scheme," in *EUROCRYPT'11*, LNCS, Springer, 2011.

[14] C. Gentry, S. Halevi and V. Vaikuntanathan, "A simple bgn-type cryptosystem from LWE," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'10)*, pp. 506–522, May 2010.

[15] C. P. Gupta, I. Sharma, "A fully homomorphic encryption scheme with symmetric keys with application to private data processing in clouds," in *NOF'13*, pp. 23-25, 2013.

[16] E. Kim, M. Tibouchi, "FHE over the integers and modular arithmetic circuits," *IET Information Security*, vol. 12, no. 4, pp. 257-264, 2018.

[17] V. Kumar, B. Buksh and I. Sharma, "Double fully homomorphic encryption for Tamper detection in Incremental documents," in *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems*, vol. 2, Smart Innovation, Systems and Technologies 51, 2016.

[18] K. Lauter, M. Naehrig, V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?," in *CCS'11*, pp. 113-124, 2011.

[19] Z. Z. Lian, Y. P. Hu, H. Chen, and B. C. Wang, "Bootstrapping of FHE over the integers with large message space," *Security and Communication Networks*, vol. 11, pp. 1-11, July 2018.

[20] C. H. Ling, C. C. Lee, C. C. Yang and M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN," *International Journal of Network Security*, vol. 19, no. 2, pp. 177-181, 2017.

[21] L. H. Liu and et al., "Computational error analysis of two schemes for outsourcing matrix computations," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 23-31, 2017.
[22] Z. H. Mahmood, M. K. Ibrahem, "New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing," in *1st Annual International Conference on Information and Sciences (AICIS'18)*, pp. 182-186, 2018.
[23] K. Nuida and K. Kurosawa, "(batch) Fully homomorphic encryption over integers for non-binary message spaces," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'15)*, pp. 537-555, Sofia, Bulgaria, Apr. 2015.
[24] M. Ogburn, C. Turner, P. Dahal, "Homomorphic encryption," *Procedia Computer Science*, pp. 502-509, 2013.
[25] M. M. Potey, C. A. Dhote and D. H. Sharma, "Low-size cipher text homomorphic encryption scheme for cloud data," 2018. (`https://doi.org/10.1007/978-981-10-4600-1_9`)
[26] R. Rivest, L. Adleman and M. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, pp. 169-180, 1978.
[27] D. Stehle, R. Steinfeld, "Faster fully homomorphic encryption," *Cryptology ePrint archive, Report*, 2010.
[28] X. D. Song and Y. L. Wang, "Homomorphic cloud computing scheme based on hybrid homomorphic encryption," in *3rd IEEE International Conference on Computer and Communications*, pp. 2450-2453, 2017.
[29] P. Zhang, X. Q. Sun, T. Wang, S. Z. Gu, J. P. Yu, W. X. Xie, "An accelerated fully homomorphic encryption scheme over the integers," in *Proceedings of CCIS'16*, 2016.

Biography

Yang Li is currently pursuing his M. S. degree from Department of Mathematics, Shanghai Maritime university. His research interests include combinatorics and cryptography.

Proposing a Secure Component-based-Application Logic and Sys-tem's Integration Testing Approach

Faisal Nabi[1], Jianming Yong[1], and Xiaohui Tao[2]

(Corresponding author: Faisal Nabi)

School of Management and Enterprise, Information Systems Research Group
Toowoomba Campus, University of Southern Queensland, Australia[1]
(Email: faisal.nabi@yahoo.com)
Faculty of Health, Engineering and Sciences, University of Southern Queensland, Australia[2]
(Email: xtao@usq.edu.au)

(Received Mar. 30, 2018; Revised and Accepted Oct. 20, 2018; First Online Jan. 21, 2019)

Abstract

Software engineering moved from traditional methods of software enterprise applications to component based development for distributed system's applications. This new era has grown up for last few years, with component-based methods, for design and rapid development of systems, but fact is that , deployment of all secure software features of technology into practical e-commerce distributed systems are higher rated target for intruders. Although most of research has been conducted on web application services that use a large share of the present software, but on the other side Component Based Software in the middle tier ,which rapidly develops application logic, also open security breaching opportunities .This research paper focus on a burning issue for researchers and scientists ,a weakest link in component based distributed system, logical attacks, that cannot be detected with any intrusion detection system within the middle tier e-commerce distributed applications. We proposed An Approach of Secure Designing application logic for distributed system, while dealing with logically vulnerability issue.

Keywords: Application Architecture; Application Logic; Component-Based-Development; Design Flaw; Logical Attack; Web Software Risk

1 Introduction

Advent of the e-Commerce ushered in a new period pervaded by sense of boundless excitement & opportunities. However, need to think of risks as mere opportunities, the reason being that, in most business environment, the number or size of the risks taken usually to the number or size of the advantages to be gained. Today, vendors of e-Commerce systems are relied solely on secure transactional protocols such as SSL, TSL Nevertheless; the advancement of the security field has proved that vendors of e-commerce systems can not solely rely on secure transaction protocols such as SSL an encryption protocol promoted as proof of 100 % security by e-commerce vendors [1, 11].

Lost in the hype are the real security risks of e-commerce security is more than secure transactional

protocols, cryptographic schemes / techniques, parameter security, Intrusion detection systems etc, these attributes make up only some part of security, privacy & client trust of e-commerce [4].

The software that executes on the either end of the transaction-server-side or client-side software poses real threats to the security, privacy in e-commerce systems. Two familiar adages play an important role in understanding to secure e-commerce systems (1) A chain is only as strong as its weakest link (2) in the presence of obstacles, the path of least resistance is always the path of choice [2]. Although, the security issues of the front-end & back-end software systems in e-commerce application warrant equal attention for complete security in e-commerce . This research paper focus is to represent the weakest link in e-commerce system which is based on CBS in middle Tier; we will also prove through experiment, logic subversion attack that cannot be detected with any intrusion detection system within the middle tier based application logic.

1.1 Contribution

Our work makes two important contributions, related to web insecure software development practices. This explained three categories of operational vulnerabilities; our target is Application Logic operational vulnerabilities that can be because of (1) design weaknesses, or (2) system configuration errors that may leads calling wrong component operation. We have proposed UML Based Secure Designing for Application Logic and system's integration testing model with applicability of system unification process for assurance purposes.

1.2 Type of Scientific Research

This research de-pends on exploratory research project that targets new idea about application vulnerability to scope out extent of business logic phenomena problem to generate idea about this phenomena. Proposing through UML based secure design modeling & system integration testing model with applicability of unification process for assurance.

2 Application Business Logic

The business logic describes the steps required to complete or perform a particular action as defined by the application developer, this is also called business logic because it contain business rules in e-commerce system in the middle tier. Modern web application implements business logic & its use changes the state of the business (as captured by the system) [12,13]. Web application executes business logic & so the most important models of the system focus on the business logic & business state, that refer to business rules as defined within an application of e-commerce to perform a particular action based on designing & implementation [12, 13, 19].

The middle tier of e-commerce servers that implements the business application logic represents the functions or services that a particular e-commerce site provides. As a result, a given site may often employ custom-developed logic. As the demand for e-commerce services grows, the sophistication of the business application logic grows accordingly [2, 4].

3 Component-Based-Software Role in Business Logic & Concerns

A framework that provide a way to distribute a self-contained piece of software in forms, called "Objects" or in generally" Components" is encapsulated in a standard that can interoperate with other components

in a framework such as JavaBeans, COM,DCOM & CORBA [2]. E-commerce sties offer more than front-end servers; however. They will usually run complex middleware programmes such as CGI, Java servlets, Application servers & Component-based-Software such as Enterprise Java Beens, Java 2 Enterprise Edition (J2EE), CORBA, COM & DCOM Components. Basically, Component-based-Software idea is to develop, purchases & reuse industrial-Strength Software in order to rapidly prototype business app-logic [17]. One of the more popular component frame works for e-commerce application is EJB, which support Component –Based Java Been. Other Component based technology models include the common object request broker architecture (CORBA) an open standard developed by OMG & Common object model by Microsoft & DCOM which support .Net environment [4].

The component frameworks are the glue that enables software components to provide services, business app-logic & uses standard infrastructure services such as naming, persistence, introspection & event handling, while hiding the details of the implementation by using welldefined interfaces [4]. The business application logic is coded in software "Components" that can be "Custom-Developed or purchased Commercial-off-the-shelf" [4]. In-addition to supporting the CGI functions, component –Based Software is expected to enable distributed B2B applications over the internet, and as that market for component–based software heats up, many standard business application logic components will be available for purchase off the shelf [4].

The application servers provide the infrastructural services for particular component models such as EJB, CORBA, COM, and DCOM. They also provide an interface for the business application logic to back-end services such as database management, enterprise resource planning (ERP), & legacy software system services [3, 4].

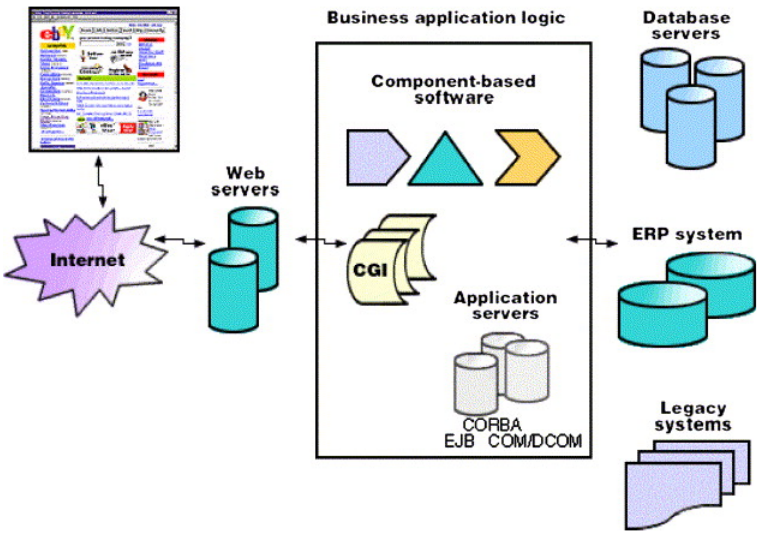

Figure 1: Component based business application logic

There is no doubt that component based software provide numerous benefits, but it poses security hazards similar to CGI scripts. CBS enables Software development in general –purpose programming language such as Java, C & C++.As these components execute with all rights & privileges of server process same, same like CGI they process untrusted user "Input" because Component based software

can be used to build sophisticated large-scale applications, errors are unarguably more likely with CBS. Regardless of the implementation Application serv-ers-the security risks of server side software are higher & therefore server-side software must be carefully designed & implemented. One reason for the emergence of Components-based-software on e-commerce sites is the complexity of the software necessary to implement business application logic. This complexity, in turn, introduces more software flaws that can be exploited for malicious gain.

4 Web Software Application & Component-Based-Development Risks

Modern web applications run large scale software applications for e-commerce, Information-distribution, Entertainment, Collaborative research work, Surveys, & numerous other activities.

They run distributed hardware platforms & heterogeneous Computer systems. The software that powers Web applications is distributed, is implemented in multiple languages & styles , incorporates much reuses & third-party components , is built with cutting edge technologies as stated (section Component based Software) & must interface with users, other web sites & databases. Although. Server-side components are relatively new to the component market. Benefits enable the developer to provide solutions that run on a per server basis. These components serve many clients simultaneously without significant performance loss. Server-side components can also be upgraded efficiently removing the complexities of updating potentially thousands of desktop machines.

Component logic is often run on powerful servers as opposed to a desktop machine [9]. This makes the server-side component an excellent candidate for systems that require efficient throughput and performance [20]. The word "heterogeneous" is often used for web software, it applies in so many ways that the synonymous term "diverse" is more general & familiar, & probably more appropriate [5]. The software components are often distributed geographically both during the development & deployment (diverse distribution), & communicates in numerous distinct & sometimes novel ways (diverse communication) [10].

Web-based-software systems by integrating numerous diverse components from disparate sources, including custom-built special-purpose applications, customized "Commercial off-the-shelf Software Components & third-party products [5]. Much of the new complexity found with web-based applications also results from how the different Software components are integrated. Not only is the source unavailable might be hosted on computers at remote, even competing organization. To ensure high quality for the web systems composed of very loosely coupled components, which seriously required evaluate these Components connections [6].

Web software Components are coupling more loosely than any previous software application(Jeff Offutt,2002).As it is stated above that e-commerce sites offer more than front-end servers, they usually run complex Middleware programmes such as CGI Scripts, Java Servlets, application Servers & Component-Based-Software such as EJB Java Beans, J2EE, CORBA, COM & DCOM Components-Based Solution. One reason for the emergence of this Component-based software on e-commerce sites is the complexity of the software necessary to implement business application logic. This Complexity, in turn, introduces the more Software Flaws that can be exploited for malicious, gain [3, 22].

The web's function & structure have changed drastically, particularly in the past couple of [5], example of a changes in last couple of years idea use of web 2.0 feature Ajax (The Ajax engine is the client-side code that handles calls between the client & server) .

Typically this would be a library of JavaScript function included on the page [7], more prone it is to have flaws in that any attacker with basic skills can use proxy software (or call script functions directly)to bypass the intended logic/business logic due to complexities involved & since more appli-

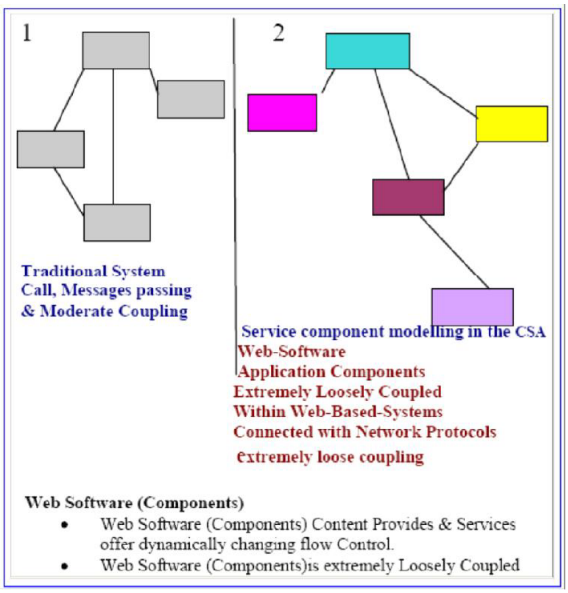

Figure 2: Traditional tightly coupled software system vs. extremely loosely coupled web software systems

cation logic is being delegated to web browser , this idea of Ajax is leading to open flaw which allows intruders to easily read the source code & look for weakness area in the system middle-tier application logic. Sharing business logic client-side reveals source information of the complete system, which is too dangerous combining representation logic, rendering logic & business logic & resides business logic client & Application server-side. For example, Ajax-enable application with multiple levels of user account it was found that the site employed one JavaScript include file for the entire client-side logic. This meant that an anonymous user with trail account could see the logic behind the administrator-level service call. The locations of all administrator service script were disclosed, providing invitation a definitive map of application to a potential attacker to attack business logic in the middle-tier, therefore, in this scenario EASI framework also get failed to protect the system integrity & security. Web sites are now fully functional software systems that provide business-to-customer e-commerce, busi-ness-to-business e-commerce & many services to many users.

The growing use of third-party software components & middleware represents one of the biggest changes in the e-commerce web software-Application systems so as Security; integrity has threat because of the Flaws in the design.

The business application logic is a key weak link in security of many online sites. Typically, application subversion attacks as well as data driven attacks exploit weakness in this web app-software.

5 Security Properties Violations in Middle Tier

The violation in the middle tier is real caused based on business rule, in a way, those are deployed, basically indicate serious violation and related Integrity & security. Component based software that develops rapidly business application logic can be Custom-Developed/COTS that may have flaws in design of its web software application. The use of component based software risks, cause of these

logical vulnerabilities that may lead towards subversion, misuse or circumvent the steps deployed by the application function.

The major cause of web insecurity is insecure software development practices. Operational security vulnerabilities generally have three main causes:

1) Design weaknesses;

2) Implementation/coding vulnerabilities;

3) System configuration errors.

Addressing design weaknesses ,especially important because these weaknesses are not corrected easily after a system has been deployed. We are working on operational vulnerabilities in the middle tier of web based information system that is composed with Components, not on traditional software techniques as used to be in the past.

As that, it is explained three categories of operational vulnerabilities, our target is Business Application Logic operational vulnerabilities that can be because of (1) design weaknesses, or (3) system configuration errors that may leads calling wrong component operation.

Unfortunately, even simple flaw in the complex middleware layer can provide the leverage necessary to bypass even strong authentication schemes. Whereas most front-end & Back-end systems are commercial-off-the shelf (COTS) software packages, a good portion of the middleware software is necessarily custom-development in order to implement every business's particular application logic.

The most significant weak link in server-side systems is the middleware layer. Therefore, a strong risk management plan will focus on providing rigorous software assurance for the middleware software [3].

"A software system's security & its integrity only as secure as its weakest component" [14].

Security problems originate from flaw in software design, and configuration management. These flaws are leveraged by the users of the software by malicious or accidently providing a level of access & privilege that would not otherwise be granted by the programme [1].

A flaw become the cause to represent vulnerability in the underlying software mitigating a flaw typically involves significantly more effort than simply modifying a few lines of code. Please note another point that problem does not solely in the implementation, the implementation that follows the design flaws & based on component-based (COTS) software that might contain the flaws. For example , the classical example, for instance performing sensitive business logic in a tainted client application is a design flaw that cannot be mitigated by simple measure such as modification array bounds.

Designing software behave, is a process that involves indentify & codifying policy & logic, then enforcing that policy & logic with reasonable technology to perform certain function or activity. There is no silver bullet for software security. Advance technology for scanning code is good at finding implementation-level mistakes, but there is no substitute for experience [15, 16].

6 Application Logic Attacks Operation

Unlike, common application technical attacks, such as SQL injection or buffer overflow, each application logic attack is usually unique, since it's not mentioned or part of any taxonomy of web application attacks, and since it has to exploit a function or feature that is specific to the application. Since, application logic attacks are not based on characteristics like buffer overflow which can be characterize them as other technical vulnerabilities in the web application (SQL, SSI or buffer overflow).This makes it more difficult for automated vulnerabilities testing TOOLS to identify or detect such vulnerability class of attacks because they are caused by the flaws in Logic & not necessarily flaws in the actual Code.

When application logic attacks are successful, it is often because developers do not build sufficient process validation & controls into application logic. This lack of functional flow control of logic allows attacker to perform certain steps incorrectly or out of order of the defined Logic.

An experiment conducted to demonstrate attacking on application's business logic in the scenario of the (SOAP) by injecting code in the SOAP message. In this case, as we know all that (SOAP) is a message-based communications technology that uses the XML format to encapsulate data. It can be used to share information and transmit messages between systems, even if these run on different operating systems and architectures. Its primary use is in web services, and in the context of a browser accessed web application, you are most likely to experience SOAP in the communications that occur between "Application Components" [8].

SOAP is often used in large-scale enterprise applications where individual tasks are performed by different computers to improve performance (W3C.org). It is also often found where a web application has been deployed as a front end to an existing application. In this situation, communications between different components may be implemented using SOAP to ensure modularity and interoperability. Because XML is an interpreted language, SOAP is potentially vulnerable to code injection in a similar way as the other examples [18].

XML elements are represented syntactically, using the "Metacharacters" <> and /. If user supplied data con-taining these characters is inserted directly into a SOAP message, an attacker may be able to interfere with the structure of the message and so interfere with the application's logic or cause other undesirable effects [19].

A "Banking Application" in which a user initiates a funds transfer using an HTTP request like the following:

```
POST /transfer.asp HTTP/1.0
Host:ask-bank.com
Content-Length: 65
FromAccount=18281008&Amount=1430&ToAccount=
08447656&Submit=Submit
```

In the course of processing this request, the following SOAP message is sent between two of the application's back-end components:

```
<soap:Envelope
xmlns:soap="http://www.w3.org/2008/2/soap-envelope"
>
<soap:Body>
<pre:Add xmlns:pre=http://target/lists
soap:encodingStyle=
"http://www.w3.org/2008/2/soap-encoding">
<Account>
<FromAccount>18281008</FromAccount>
<Amount>1430</Amount>
<ClearedFunds>False</ClearedFunds>
<ToAccount>08447656</ToAccount>
</Account>
</pre:Add>
</soap:Body>
</soap:Envelope>
```

Look how the XML elements in the message correspond to the parameters in the HTTP request, and also the addition of the ClearedFunds (Component). At this point in the application's logic, it has determined that there are insufficient funds available to perform the requested transfer, and has set the

value of this Component to False, with the result that the component which receives the SOAP message does not act upon it. In this situation, there are various ways in which you could seek to inject into the SOAP message, and so interfere with the application's logic. For example, submitting the following request will cause an additional ClearedFunds (Component) to be inserted into the message before the original element (while preserving the SQL's syntactic validity). If the application processes the first ClearedFunds (Component) that it encounters, then you may succeed in performing a transfer when no funds are available:

```
POST /transfer.asp HTTP/1.0
Host: ask-bank.com
Content-Length: 119
FromAccount=18281008&Amount=1430</Amount><Cl
earedFunds>True</ClearedFunds><Amount>1430&To
Account=08447656&Submit=Submit
```

If, on the other hand, the application processes the last ClearedFunds (Component) that it encounters, you could inject a similar attack into the ToAccount parameter.

A different type of attack would be to use XML com-ments to remove part of the original SOAP message altogether, and replace the removed elements with your own. For example, the following request injects a ClearedFunds (Component) via the Amount parameter, provides the opening tag for the ToAccount (Component), opens a comment, and closes the comment in the ToAccount parameter, thus preserving the syntactic validity of the XML:

```
POST /transfer.asp HTTP/1.0
Host: ask-bank.com
Content-Length: 125
FromAccount=18281008&Amount=1430</Amount><Cl
earedFunds>True</ClearedFunds><ToAccount><!--
&ToAccount=-->08447656&Submit=Submit
```

A further type of attack would be to attempt to complete the entire SOAP message from within an injected parameter and comment out the remainder of the message. However, because the opening comment will not be matched by a closing comment, this attack produces strictly invalid XML, which will be rejected by many XML parsers:

```
POST /transfer.asp HTTP/1.0
Host: ask-bank.com
Content-Length: 176
FromAccount=18281008&Amount=1430
<Amount>
<ClearedFunds>True</ClearedFunds><ToAccount>084
47656</ToAccount></Account></pre:Add></soap:Body
></soap: Envelope><!--&Submit=Submit.
```

In most situations, you will need to know the structure of the XML that surrounds your data, in order to supply crafted input which modifies the message without invalidating it. In all of the preceding tests, look for any error messages that reveal any details about the SOAP message being processed. This will disclose the entire message, enabling you to construct crafted values to exploit the vulnerability.

Experiment Result:

Hence, we have derived the result from this experiment, that application's component logic can be subverted, even if, application follows absolutely correct functionality. This course of action proved the

claim that such attack subversion of application logic cannot be detected, even if EASI frame work of security deployed, failed to filter or catch this security breach attempt. Through this experiment research, it is concluded that business logic layer in n-tier applications need for such a design strategy is motivated by the fact that logical flaws do not show patterns or signatures and, thus, their discovery cannot be automated.

7 Previous Model of Security EASI for e-Commerce System

Actually previous model EASI does not meet the com-plete solution since it's also based on COTS Security Products these security services are used through API,s of Security services as mentioned within the Model EASI [21] provides a common security framework to integrate many different security solutions to securely connecting Web servers to back-office data Stores. The key security services of this model authentication, authorization, cryptography, accountability, and security administration.

Therefore, since the nature of business application logic vulnerabilities are varied, as explained above in the experiment and in Section 6.1,7, which is reason why explained above EASI framework does not control those problems in the business application logic to be attacked or violation its integrity & logical functions.

8 Proposed UML Based Secure Designing for Application Logic

One of the first steps in system design should be the analysis of the possible attacks to the specific system and their consequences when successful. This analysis can be used to define the countermeasures that need and will also be useful later to evaluate the system security.

Identifying the components that needs to be secured, is a very important factor and first stage in the designing a secure environment for system. Next mechanisms that can be used to secure those components need to be identified. It is then necessary to understand which mechanisms are to be put together to secure the components thus giving rise to a secure development scenario.

In the n-tier distributed–computing environment, front-end presents presentation logic which invoke the business logic for the submitted request then the business logic layer hosted application interacts with the data tier & its logic for requested enquiry and computes the results that will be delivered to the presentation-logic layer.

Typically , security senility increases its flow from the first layer towards the last such partitioning into zones helps define the security requirement for the environment & the design of the topology to the host the components. It is also need to make sure that every aspect of the application's design is clearly mentioned in the sufficient detail to understand every assumption made by the designer and all such assumption must be explicitly on the record within design plan.

For example, sources code is clearly commented purpose & intended uses of each component and assumption made by each component about anything that is outside of its direct functional control. It is also important to reference to all client code which makes use of the component and clear to it effect could have prevented the Logic flaw within the online registration functionality as defined in the example in that case "client" here refers not to the user end of the client-server relationship but to other code for which the component being considered is an immediate dependency. When implementing functions that update session data on the basis of input received from the user or actions performed by the user, reflect carefully on any impact that the updated data may have on other functionality within the application unexpexted side effects can occur in entirely unrelated functionality defined by a different programmer or even a different development team.

8.1 UML Based J2EE Secure Design Modeling for Application Logic

Designing of application for e-commerce distributed system in a tier is also very important since many attacks are cause of design flaws in the e-commerce systems such logical flaws do not often refer to component based flaws but also architectural, component modeling to set the logic of application while using business rules related to the particular business or activity. Therefore , it is very important to define clearly architectural design of topology in which system going to design for deploy by separating each tier clearly , second stage focus on the appli-cation logic design strategy & policy with that components have to function under given business defined rule/policy , third stage refer to design strategy for components which dynamic web content is used to tailor an individual's interactions with a web site & provide users with more interactive information. Dynamic content may be rendered in various form, such as static HTML files, Java Script or JSP file rendered using component supported environment such as Java servlets in a J2EE invokes business –logic application hosted middle tier to access back-end business data.

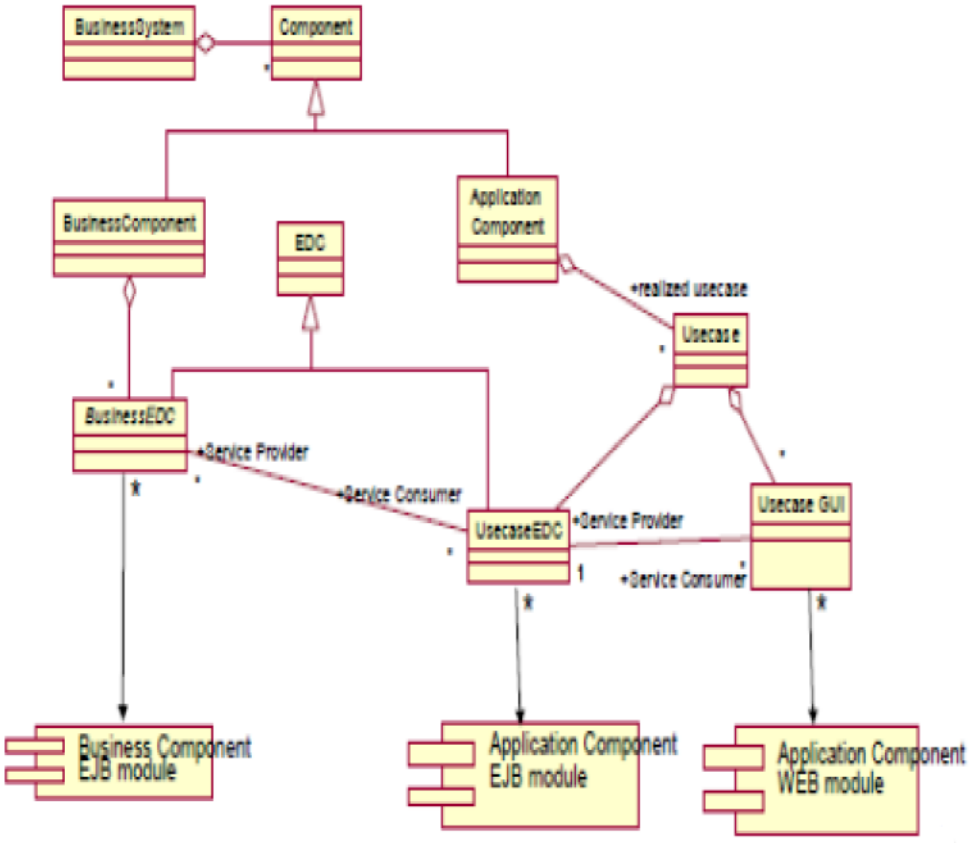

Figure 3: UML based secure design J2EE component based application logic modeling

In the above given example of attack as it is stated that always follow right principles of web application software engineering in the right technology environment support for component interoperability & security. it is noticed in the example that threat to the application integrity & application dependability based on the design flaw & engineering of the component while defining logic for e-commerce system

web application software by merging all logic and invoke the direct access using servlets through JDBC to the back-end having bypass the middleware process or without encapsulating the business logic in an enterprise bean, it also define screening as a shield to the organizational resources by restricting unauthorized people to access valuable data or temper the resources.

8.1.1 Validation for the proposed UML Based Secure Design J2EE Component Based Applica-tion Logic

Business-level- Process Integration is based on business component's integration, which takes part to process a certain job/task event. This comes into being because of business logic inside a component. When we talk about business process integration, it means integrating business component's business processing logic, this integration completely rely upon "Business" component's Interface. A component interface is self-descriptor that provides specification, which defines component offers, what service such as, Account service provided by Account Component interface (as given above example experiment study), this is called Component interface specification, it reflects component's business process functionality, and indicates a component offer a particular service [24].

By using this specification, we can derive a component's syntax and semantics to determine its provided and required interfaces. The provided interface is a collection of functionality and behavior that collectively define the service a component provides to its associated clients. It may be seen as the entry point for controlling the component, and it determines what a component can do. If we look at a component from the point of view of its provided interface, it takes the role of a server. If we look at it from the point of view of its required interface, the component takes the role of a client. Provided and required interfaces define a component's provided and required contracts [25].

8.1.2 Integration and System Testing Approach

Components and integration level testing is therefore often confronted with the problem that the service provided by the component or a group of components under test (the SUT) requires functionality of components which are not ready for integration. Delays of the component and integration level testing process can be avoided by the development of emulators for the missing functionality and an elaborated project plan which considers the integration order of the components. This integration level testing shows, how the UML Testing Profile (UTP by (OMG)) can be utilized for this kind of testing [23].

Since model-based integration and system testing does not require all component realizations .Models can usually be available earlier than realizations, this model-based I & T technique enables earlier detection and prevention of problems when compared or matched to real system testing.

Furthermore, models usually allow easier adaptation and configuration than realizations, which means that they are well suited for system testing under different conditions. Especially for exceptional behavior testing, creating the non-nominal test conditions, e.g., a broken component, is usually easier and less expensive when models are used instead of realizations. Besides that this improves the coverage and thus the quality of tests, the ability to rapidly change test conditions using models also improves the efficiency of test execution. As such, model-based system testing not only allows earlier testing, but it also increases the risk reduction rate for the test phase.

Figure 4 contains a graphical representation of mod-el-based integration and system testing. When only the depicted components C1 and Cn are considered, the figure shows that component C1 is represented by model M1, while component Cn is represented by realization Zn. Using the model-based integration infrastructure IMZ, model M1 and realization Zn are integrated, yielding the model-based integrated system {M1, Zn} IMZ.This early representation of the system is then tested on the system level using tests derived from the system requirements R and the system design D, which is graphically represented by the dashed arrow .

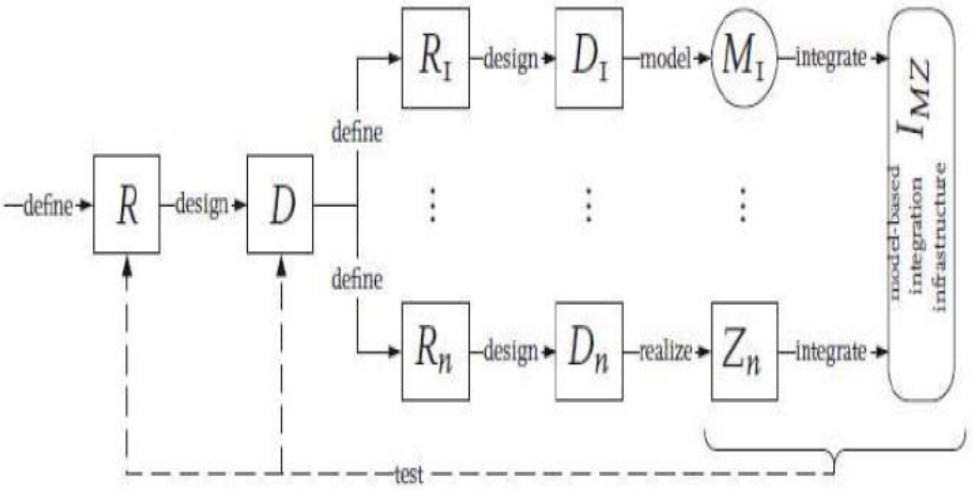

Figure 4: Integration and system testing model

8.2 Systems Unification Approach for Application Process & Assurance Properties

In cooperating our design model through model-based approach in component-based-software development, would promotes as a means to achieve cost-effective, high quality of assurance in the development and platform-independent design. This approach is a means of realizing the "correct by construction philosophy" where by flaws in a product design are discovered early at the design stage, such as components integration flaws. By using this approach, we can extract the integration flaw/fault existing between the components interfaces, interacting with each other in the system, that is composed with the component's integration on the bases of their "business process functionality".

Component's realization contract artifacts help to understand design and applicability of its transformation into model-based application process for assurance properties unification that can be achieved by its interconnection relationship behavioral study.

Application of extracted test design for an e-commerce system should follow a complete plan.

1) Scenario-based-approach for modeling business scenario to generate test scenarios from extracted Test design.

2) Selecting integration strategies of components matching with requirement specifications & their offered and used interface, design drivers and stubs.

3) Derive test scenarios from business scenarios and business flows of components, and derive test cases by analyzing business data. Limits of Conducted Practice:

The above proposed secure design strategy successfully, practiced at above mention e-commerce industry. Due to ethical right and their company policy, snapshots of integration or component test (Diagnostic specification) out come not allowed exposing publically.

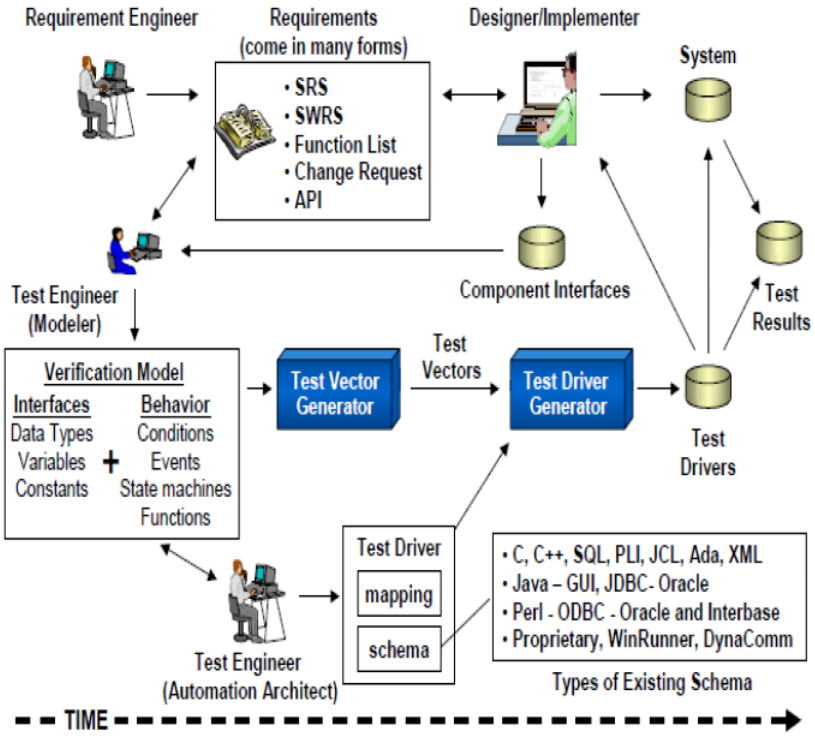

Figure 5: System s unification approach for application process & assurance properties

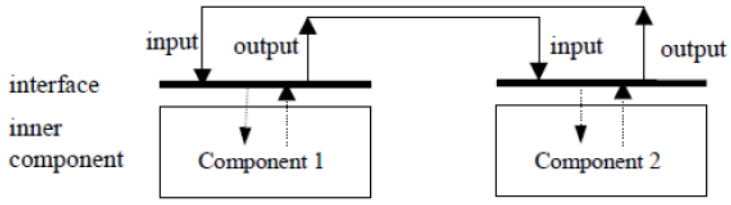

Figure 6: Component's interconnection relationship design by contract

9 Conclusion

Attacking an application's logic involves a mixture of systematic probing and lateral thinking. As we have identified, there are various key points' checks that one should always carry out to the application's behavior.

Often, the way an application responds to these actions will point towards some defective assumption that can violate, to malicious effect.

Therefore, common sense is a appropriate tool while designing secure web application software and deploying component based business logic into the system. Application system developer must focus on security besides the functionality, because this functionality can be productive, when it works as per and within its functional control defined business policy into the e-commerce systems.

References

[1] A. K. Ghosh, *E-Commerce Security: Weak Links Best Defence*, John Wiley & Sons, New York, 1998.
[2] A. K. Ghosh, *Security and Privacy in Ecommerce*, John Wiley & Sons, 2000.
[3] A. K. Ghosh, *Security & Privacy for EBusiness*, John Wiley & Sons, 2001.
[4] F. Nabi, "Secure business application logic for e-commerce systems," *Elsevier Journal of Computers & Security*, 2005.
[5] J. Offutt, "Quality attributes of web software applications," *IEEE Software*, vol. 19, no. 2, pp. 25-32, 2002.
[6] E. Dustin, J. Rashka, D. McDiarmid, *Quality Web System: Performance, Security & Usabilty*, Adition-Wesley, Boston, 2001.
[7] P. Ritchie, The Security Risks Of Ajax/Web 2.0 Application, Elsevier, Network Security, 2007.
[8] C. V. Berghe, J. Riordan, F. Piessens, "A vulnerability taxonomy methodology applied to web services," *IBM Zurich Research Laboratory*, 2005.
[9] R. R. Raje, B. R. Bryant, M. Auguston, A. M. Olson, C. C. Burt, "A unified approach for the integration of distributed heterogeneous software components," in *Proceedings of Monterey Workshop Engineering Automation for Software Intensive System Integration*, 2001.
[10] F. Cao, B. R. Bryant, R. R. Raje, M. Auguston, A. M. Olson, and C. C. Burt, "Component specification and wrapper/glue code generation with two-level grammar using domain specific knowledge," *Lecture Notes Computer Science*, vol. 2495, Springer-Verlag, 2002.
[11] G. Simson, S. Gene, *Web Security And Commerce*, O'Reilly Publishing, 1997.
[12] M. Hung, Y. Zou, *Extracting Business Process From The Three-Tier Architecture System*, Queen's University Kingston, ON, K7L 3N6, Canada 2005.
[13] M. Hung and Y. Zou, "A framework for exacting workflows from e-commerce systems," in *Proceedings of Software Technology and Engineering Practice*, 2005.
[14] J. Viega, G. McGraw, *Building Secure Software*, John Wiley, 2006.
[15] G. Hoglund, G. McGraw, *Exploiting Software*, Adition-wesley, 2004.
[16] D. Verdon, G. McGraw, "Risk analysis in software design," *IEEE Security & Privacy*, vol. 2, no. 4, pp. 79-84, 2004.
[17] D. Allan, *Web Application Security: Automated Scanning or Manual Penetration Testing*, Jan. 2008. (`ftp://ftp.software.ibm.com/software/rational/web/whitepapers/r_wp_autoscan.pdf`)
[18] M. McIntosh and P. Austel, "XML signature element wrapping attacks and countermeasures," in *Workshop on Secure Web Services*, 2005.
[19] M. A. Rahaman, A. Schaad, and M. Rits, "Towards secure soap message exchange in a SOA," in *Workshop on Secure Web Services*, 2006.

[20] G. J. Brahnmath, R. R. Raje, A. M. Olson, M. Au-guston, B. R. Bryant, C. C. Burt, "A quality of service catalog for software components," in *Proceedings of the Southeastern Software Engineering Conference*, 2002.
[21] R. Heffner, *Planning Assumption: Giga's Model for Enterprise Application Security Integration*, Giga Information Group, June 22, 2001. (`http://www.gigaweb.com`)
[22] D. Schmidt, M. Stal, H. Rohnert, F. Buschmann, *Pattern-Oriented Software Architecture*, Vol. 2, Patterns for Concurrent and Networked Objects, Wiley, 2000.
[23] P. Baker, *et al.*, *Component and Integration Level Testing*, Springer Belin Heidelberg, 2007.
[24] M. Juric, R. Nagappan, R. Leander, S. J. Basha, *Professional J2EE EAI*, Wrox Press, 2002.
[25] H. G. Gross, *Component-Based-Software Testing with UML*, Springer, 2005.

Biography

Faisal Nabi is a PhD researcher at university of southern Queensland Australia. He has published some interesting papers on component-based application logic vulnerability. His main area of research is e-commerce security, specially focus on rapidly developed COTS based application design (security by design).

Jianming Yong is an Associate Professor at University of Southern Queensland.He did his PhD from SwinburneUT. His main area of research interest are Advanced Networking, Internet technology, M-Commerce,E-business, Data Integration, Workflow systems, Information system security, Network management. He is member of IEEE.

Xiaohui Tao is Senior Lecturer in Faculty of Health, Engineering and Sciences, University of Southern Queensland (USQ), Australia. Before joined USQ, I was a Research Associate with the e-Discovery Lab, Faculty of Science and Technology at Queensland University of Technology (QUT), Australia, and completed PhD in QUT as well.His research interests include Information Retrieval, Text Mining, and Knowledge Engineering.

Artificial Intelligence in Nigeria Financial Sector

Richman Charles Agidi
(Corresponding author: Richman Charles Agidi)

Houdegbe North American University Benin
06 BP 2080, Route de Porto Novo Cotonou, Agblangandan, Benin
(Email: richykleen1st@gmail.com)

(Received Jan. 18, 2019; Revised and Accepted Feb. 9, 2019; First Online Feb. 10, 2019)

Abstract

Artificial intelligence has revolutionized the financial industry and deploying Artificial Intelligence in Nigeria Financial Industry will unlock significant opportunities that would transform retail lending, product design, and the overall banking model to the mass market. The need for AI in Financial Industry with the conditions of the favorable technology, that involves (1) Interaction of speech recognition software, mobility tracking systems such as GPS and Wi-Fi, and even gesture interpretation. (2) Intelligence developments in machine learning are opening the way for advanced applications. (3) Data, on which the amount of data is set to grow even faster in Financial Industry, since Artificial Intelligence is fed by data.

Keywords: AI; Big Data; Blockchain; Financial Industry

1 Introduction

Artificial intelligence is such a broad category that it defies simple description, but typically refers to a suite of modelling techniques that bring together some combination of the following: huge data sets, non-traditional (i.e., including unstructured and changing) data, demonstrating complex relationships between variables sometimes result in opaque ("black box") models, and models with rapidly time-varying structures. As AI provides previously unknown insights, banks are implementing AI models in order to increase revenue or reduce cost through better and faster decision-making. Customer segmentation, fraud detection, price optimization, compliance monitoring, and loss forecasting are only a few examples of areas where financial institutions have built models using a range of approaches such as clustering algorithms, deep neural networks, and sentiment analysis [31].

The Financial Stability Board (2017) defines Financial Technology as "technologically enabled financial innovations that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and on the provision of financial services" [9], this progress in technology is also propelled by the enormous volume of data from customers and market players with the automation as well as digitalization of financial services – banking, insurance and trading. Data explosion is clearly the key-enabler [15]. The opportunities for the application of AI in banking are immense and we expect the effect to grow significantly in the next few years. Research by the international Data Corporation forecasts that globally, AI solutions will continue to

see significant corporate investment over the next several years, achieving a compound annual growth rate of 54.4% through to 2020 [29]. Artificial intelligence will enable financial services companies to completely redefine how they work, how they create innovative products and services, and how they transform customer experiences [13].

Blockchain, Artificial Intelligence, Big data, Adoption of Artificial Intelligence and development in financial Industry. Artificial intelligence (AI), often called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans and other animals. Financial institutions have long used artificial neural network systems to detect charges or claims outside of the norm, flagging these for human investigation. The use of AI in banking can be traced back to 1987 when Security Pacific National Bank in US set-up a Fraud Prevention Task force to counter the unauthorized use of debit cards. Programs like Kasisto and Money stream are using AI in financial services [10].

2 Blockchain

According to Global Fintech Report 2017, 77% of Fintech institutes expect to adopt blockchain as part of an in the production system or process by 2020. Blockchain provides a very high level of safety and security when it comes to exchanging data, information, and money. It also allows users to take advantage of the transparent network infrastructure along with low operational costs with the aid of decentralization. These characteristics make Blockchain reliable, promising and in-demand solution for the banking and finance industry [21] (See Figure 1).

Figure 1: Applications of blockchain in finance

Blockchain with the main application to crypto-assets, with main risks arising from fraud detection, money laundering risk, IT operational risk and cyber risks [8]. The World Economic Forum estimates that, by 2017, 80% of all Banks are going to initiate projects concerning Distributed Ledger Technology (DLT)–the underlying technology supporting a Blockchain. In the past 3 years, Fintech startups working on Blockchain have attracted venture capital funding of over $1.4 Billion. During the same period, over 2500 patents have been filed and over 90 Central Banks are presently engaged in DLT related

discussions worldwide [19]. Since 2015, a number of major international financial institutions have begun to formulate plans for the blockchain sector. Goldman Sachs, J.P. Morgan, UBS, and other banking giants have all established their own blockchain laboratories, working in close collaboration with blockchain technology [9].

Blockchain technology is based on the concept of sharing information across different parties and consensus during transactions, and thereby helps in saving on reconciliation cost between banks [19]. This also helps in preventing losses because of documentary frauds [3]. Blockchain's disruptive nature is derived from its ability to transform almost any process, from basic documentation, to settling complex contracts across geographies. This inherent capability is alluring to finance and banking, decision-makers, who believe its disruptive power is good for their industry [25]. Recently, the banking industry has started investing in a wide range set of projects and start-ups providing blockchain based solutions as this technology provides a high level of safety for storing and transmitting data, distributed and transparent network infrastructure, decentralization and low cost of operations [22].

Banks have increased conducting tests of decentralized asset technology and implementing blockchain in the business process. As blockchain itself holds an immutable ledger that records all transactions in the chain, if a large number of transactions are being processed by the network, a huge volume of data gets collected and AI techniques can be used to process and classify the data. Telcoin [26], the feature of blockchain smart contracts gives the ability to program the blockchain to govern transactions among participants involved in decision making or generating and accessing the data [13]. Most credit and financial institutions cannot carry out their work without a number of mediators, while their participation make the services of these institutions much more expensive. The implementation of blockchain will enable unnecessary mediators to be abandoned and provide customers and banks with cheaper services [27].

3 Big Data

The financial services industry is spending to enable itself to parse big data, extract the preferences and spending habits of each individual customer and drive the personalization of services." [30]. This banking and financial industry is one of the biggest adopters of big data technologies; Banks internationally have started to harness the power of data to derive utility across various parts of their functioning. Big data in financial industry is defined as tool that allows an organization to create, manipulate, and manage large sets of data in a given time and the storage that supports such voluminous data [4], analyzing big data allows analysts, researchers, and business users to make better and faster decisions using data that was previously inaccessible or unusable [11].

Switching to Big Data will allow them to process this information faster, avoiding any potentially embarrassing situations; it will allow the banking industry to track customers' credit card and loan limits, ensuring that they don't over spend [17]. There is huge potential for banks to realize value from the data available to them. It has been said that data is the new oil. AI is a natural fit for"mining" this data and extracting value for the banks. Banks globally have begun to utilize AI across the banking value chain to grow revenue, reduce costs, increase productivity and gain strategic insight. It appears that the AI technology market is dominated by a few giant players: IBM, Google, Microsoft and Intel from the US and Baidu, Alibaba, and Tencent ("BAT") from China. There is a feeling of déjà vu since the same situation exists in the digital platform economy–few companies dominate the market and basically have monopolies in their specific fields [2].

4 Adoption of Artificial Intelligence in Financial Industry

Artificial intelligence (AI) adoption, its benefit are already being realized at many large banks across the globe. According to Tata Consultancy Service (TCS) research, ''banking and FS executive found that investment in AI helped them reduce production costs by 13% [26]. UBS used the help of artificial intelligence when delivering personalized advice to the bank's wealthy clients by modeling 85 million Singaporean individual's behavioral patterns [19].The adoption of AI in the banking and finance sector in Nigeria is a part of the larger digital wave occurring within the sector. The use and deployment of AI in consumer banking, financial products and back-end operations is varied and across different stages of operations. Though it is not always clear from publicly available information the exact type of AI technology [18], and the implementation of AI by the seven leading commercial banks in the U.S. as ranked by the Federal Reserve. Changes in the banking industry directly impact businesses and commerce, in the convergence of AI and financial technology.

5 AI Development in Nigeria Financial Industry

AI algorithms rely on data or information to learn, infer, and make final decisions. The machine learning algorithms work better when data are collected from a data repository or a platform that is reliable, secure, trusted, and credible. Blockchain serves as a distributed ledger on which data can be stored and transacted in a way that is cryptographically signed, validated, and agreed on by all mining nodes [22]. To gain a competitive edge, financial services companies need to leverage big data to better comply with regulations, detect and prevent fraud, determine customer behavior, increase sales, develop data-driven products and much more [31].

This digitization of financial transactions has led to the steady accumulation of massive amounts of financial and personal data. Today, the financial industry is actively seeking ways to leverage this data to deliver new and improved services [14]. AI opportunities in financial services are broad-based addressing needs in risk assessment, financial analysis, portfolio management, credit approval process, know your client (KYC) & anti-money laundering (AML) systems, various operational and customer interaction processes and system/data security [6], Artificial intelligence can develop Nigeria Financial Industry in the following ways.

5.1 Differentiated Customer Experiences

As digital capabilities mature, new technologies emerge and customer expectations continue to evolve, banks are extending their transformation efforts from digitizing narrowly targeted functions to the broader digitization of the enterprise [5], new consumer functionalities are being built on existing payment systems and will result in meaningful changes in customer behavior [12].

Digital bank business models combine frictionless user experiences, deep analytics, scalable cloud-based platforms and agile transformation methodologies to achieve customer centricity, efficiency, resiliency and stability [12]. In addition, artificial intelligence transformations of other industries made customers more trusting of and comfortable with artificial intelligence financial solutions. It also increased their demand for immediacy and customized products and services. Some of the most prominent companies are meeting these consumer demands with low cost, convenient ways to transfer money, borrow, and invest. Client interactions may increasingly be carried out by AI interfaces with so-called 'Chabot's,' or virtual assistance programs that interact with users in natural language. This section considers each in turn [23].

5.2 Price Regulations, Marketing and Managing Insurance Policies

The insurance industry is using AI and machine learning to analyze complex data to lower costs and improve profitability. Since analyzing data to drive pricing forms the core of insurance business, insurance-related technology, sometimes called 'InsurTech,' often relies on analysis of big data. Adoption of AI and machine learning applications in InsurTech is particularly high in the United States, UK, Germany and China [23].

5.3 Mitigation of Identity Theft, Fraud and Cyber Crime

AI is being utilized to proactively monitor and prevent various instances of fraud, money laundering, malpractice and the detection of potential risks [24], biometric authentication Identity and access management coupled with IoT, enable bank managers and security officers to receive automated alerts about suspicious customer activity to protect against identity theft and fraud [28], Biometric identification of employees performing transactions on the back end is a crucial step to ensuring identity protection and reducing fraud. Biometrics in banking will help financial institutions to prevent insider fraud by establishing secure employee authentication, accountability and concrete audit trail of each transaction [1].

According to a survey conducted "Of our survey respondents, 32 percent of the group confirmed using AI technologies such as predictive analytics, recommendation engines, voice recognition and response" [7]. There is now a significant need to reduce a high degree of dependence on traditional TMS – which are slow to adapt to the dynamic nature of money laundering. AI techniques such as behavioral modeling and customer segmentation can be used to discover transaction behaviors with a view to identifying behavioral patterns of entities and outlier behaviors that detect potential laundering [16]. The Monetary Authority of Singapore (MAS) is exploring the use of AI and machine learning in the analysis of suspicious transactions to identify those transactions that warrant further attention, allowing supervisors to focus their resources on higher risk transactions. Investigating suspicious transactions is time consuming and often suffers from a high rate of false positives, due to defensive filings by regulated entities [23]. MasterCard has also worked to include AI technology as a part of their financial service network as a way "identifying identities" [24].

5.4 Enhancing Financial Advisory Services

Historically, providing financial advice has been a process driven by developing a personal relationship between a client and their financial consultant Initially, robo-advisers were viewed as a low-cost way to attract individuals who did not yet have enough money to make individual personal management worthwhile. Today, increasing numbers of consumers are more comfortable interacting with computer systems to address their needs, and most financial companies including Morgan Stanley, Goldman Sachs, Wells Fargo and Bank of America's Merrill Lynch unit, J.P. Morgan, E*Trade, Schwab, TD Ameritrade are pursuing rob-advisor service strategies [5], as the pressure increases on financial institutions to reduce their rates of commission on individual investments, machines may do what humans don't- work for a single down payment.

Regarding automated advice, 76% of our respondents believe that automated advice will grow in capabilities and sophistication and will increasingly find adoption beyond the mass affluent channel. "Robo" should not be thought of only as a channel limited to mass affluent clients, but one that will grow in sophistication and application to core high-net-worth (HNW) clients, and 68% believe that "robo" as a channel should be increasingly integrated into the advisor practice as an enabling tool [20].

5.5 Portfolio and Wealth Management

Artificial intelligence to analyze data and draw patterns that can help potential investors choose the right product for their portfolio, and give insights on price fluctuations in the future. AI-based systems analyzing a user's salary, saving, and spending to formulate an efficient financial plan that caters to their needs [18], bring 'banking at your fingertips' for the users who just hate to visit the banks. It strengthens the mobile banking facility by managing basic banking services. Customers can get the benefits of automated and safe transactions. They get notification instantly for any suspicious transaction as per their usual patterns [15].

6 Conclusions

Globally financial industries have begun to utilize Artificial intelligence across the banking value chain to grow revenue, reduce costs, increase productivity and gain strategic insight. Financial industries in Nigeria are already adopting elements of AI technologies including software robots to streamline & automate processes and catboat's that on more advanced platforms use AI to provide human-like interaction and dynamic banking services via chat conversations and will significantly reduce cost to serve each customer allowing banks increase coverage to the unbanked and boost profitability while providing excellent customer service at a progressively reducing cost. AI has the potential to disrupt their business and make the important decisions of how and where to invest in AI-based technologies. This requires understanding the AI technologies and then analyzing the bank's existing operating model (including business processes, talent models, legacy systems, data assets, and markets) in order to identity how to obtain the maximum benefit. I sincerely hope Nigeria financial industry find this research useful in crafting their organization's AI adoption strategy, financial industries could use Artificial intelligence to build or redesign their operating models and processes.

This research study adopts a qualitative approach where previous studies related to artificial intelligence were analyzed and discussed. This study is completely based on the literature review and the findings and suggestions were recommended based on the analysis review. Various studies related to Artificial intelligence in the past were considered and critically evaluated in the context of artificial intelligence in the financial industry to develop the research of the study.

References

[1] R. C. Agidi, "Biometrics: The Future of Banking and Financial Service Industry in Nigeria," *International Journal of Electronics and Information Engineering*, vol. 9, no. 2, pp. 91-105, 2018.

[2] H. Ailis, *Tools for Artificial Intelligence Discussion*, Policy Brief, pp. 1-9, 2018. (`https://tietokayttoon.fi/documents/1927382/2116852/27-2018-Tools+for+Artificial+Intelligence+Discussion/91969fa1-e4ff-434b-bce4-1de37fc379b6/27-2018-Tools+for+Artificial+Intelligence+Discussion.pdf?version=1.0`)

[3] M. C. Cauchi, S. M. Azzopardi, *Blockchain and Banking*, Chetcuti Cauchi Advocates Inc., pp. 1-5, 2017.

[4] P. Chunarkar-Patil, A. Bhosale, "Big data analytics," *Journal of Sciences*, vol. 2, no. 5, pp. 326-335, 2018.

[5] P. Davis, J. Hershey, *Tech Innovations Driving Change at US Banks*, Ernst & Young LLP, June 2016.

[6] P. Dravis, "Artificial Intelligence in Finance: The Road Ahead," in *Future Perfect Machine*, San Francisco, CA, pp. 1-21, 2018.

[7] S. Frankel, *The Rise of AI in Financial Services*, Research Bried, Narrative Science, Nov. 2018.

[8] P. Giudici, "A research challenge for artificial intelligence in finance, fintech risk management," *Artificial Intelligence*, vol. 1, no. 1, pp. 1-6, 2018.
[9] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, no. 24, pp. 1-12, 2016.
[10] S. M. Gupta, "How MasterCard is reinventing itself in the age of digital payments and artificial intelligence," Nov. 2017. (`http://in.pcmag.com/digitalpayment/117656/feature/howmastercard-is-reinventing-itself-in-the-age-of-digital-p`)
[11] IBM, "Employ the most effective big data technology," Oct. 2018. (`https://www.ibm.com/analytics/hadoop/big-data-analytics`)
[12] R. Jesse McWaters, *An Industry Project of the Financial Services Community*, Prepared in collaboration with Deloitte Final Report, 2015.
[13] R. Jubraj, T Graham, E Ryan, *Redefine Banking with Artificial Intelligence*, The Intelligent Bank. Accenture, 2018.
[14] F. Kenji, "FinTech That Accelerates Digital," *NEC Technical Journal*, vol. 11, no. 2, pp. 1-6, 2016.
[15] P. Koning, *Artificial Intelligence (AI) for Financial Services*, White Paper for Stakeholder Engagement, 2016.
[16] A. J. Kreshock, *AI Strategies in Financial Services*, Executive Brief, H20.ai, June 2018.
[17] Mauricio, "The role of big data in the banking industry," May 2016. (`https://bigdata-madesimple.com/role-big-data-bankingindustry/`)
[18] S. Mohandas, *AI in Banking and Finance*, Looking Forward Event Report 7th, The Centre for Internet and Society, India, 2018.
[19] T. V. Narendran, S. P. Monish, *Banking on the Future*, Vision 2020, CII-Deloitte, 2015.
[20] M. Perera, *Wealth Management: How Digital and Learning Algorithms Advance Holistic Advice*, Digital Business, Cognizant, Sept. 2018.
[21] M. Pratap, "How is Blockchain Revolutionizing Banking and Financial Markets," Aug. 2018. (`https://hackernoon.com/how-is-blockchain-revolutionizinging-and-financial-markets-9241df07c18b`)
[22] K. Salah, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 4, pp. 1-24, 2018.
[23] J. Schindler, *Artificial Intelligence and Machine Learning in Financial Services Market Developments and Financial Stability Implications*, Financial Stability Board, Nov. 2017.
[24] T. Sloane, "The 18 Top Use Cases of Artificial Intelligence in Banks," Nov. 2016. (`https://www.paymentsjournal.com/the-18-top-usecases-of-artificial-intelligence-in-banks/`)
[25] A. Tandulwadikar, *Blockchain in Banking: A Measured Approach*, Cognizant Reports, 2016.
[26] Telcoin, "How artificial intelligence can support blockchain applications like telcoin," Oct. 2017. (`https://medium.com/@telcoin/how-artificial-intelligence-can-support-blockchain-applications-like-telcoin-1c5bab8a1a68`)
[27] Universa, "Blockchain is Reshaping the Banking Sector," June 2018. (`https://medium.com/universablockchain/blockchain-is-reshaping-the-banking-sector-fd84f2f9c475`)
[28] W. Wang, *3 Top Big Data Use Cases in Financial Services*, EBook, Datameer, Oct. 2015.
[29] K. Wiggers, "Artificial Intelligence in Banking - Series," Aug. 2018. (`https://www.proshareng.com/news/Fintech/Artificial-Intelligence-in-Banking---Ser/41405`)
[30] J. Wilmer, "Big Data in the Financial Services Industry," Oct. 2018. (`https://www.wilmerhale.com/en/solutions/big%20data`)
[31] O. Wyman, *Managing Next Generation Artificial Intelligence in Banking*, New Paradigm For Model Management, 2017.

Biography

Richman Charles Agidi is a Nigerian and currently studying Computer Engineering Technology [B.SC] at Houdegbe North American University Benin. Benin Republic. (E-mail: richykleen1st@gmail.com)

Guide for Authors
International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:
For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.