Journal of Sensors, IoT & Health Sciences
ISSN: 2584-2560
Vol.02(02), June 2024, pp.16-29

Research Article

Secure Deep Learning Architecture Model for Data Management and Scheduling of E-Commerce Data

Hemalatha P[1,*]
[1]Assistant Professor, TIFAC-CORE in Cyber Security, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, 641112, India.
[*]Corresponding Author: Hemalatha P. Email: phemalatha@cb.amrita.edu

Received: 05/05/2024; Revised: 28/05/2024; Accepted: 22/06/2024; Published: 30/06/2024.
DOI: https://doi.org/10.69996/ jsihs.2024007

Abstract: E-commerce refers to the buying and selling of goods and services online, including everything from clothes and electronics to food and household items. It typically involves online transactions, such as payments and delivery. E-healthcare, on the other hand, refers to the delivery of healthcare services and information through electronic means, such as the Internet, mobile devices, and telemedicine. Conventionally, healthcare systems using E-commerce are subjected to challenges associated with security, Regulatory Compliance, Quality, Payment, limited accessibility and adoption. Security in the E-commerce platform is achieved with the Intrusion Detection System (IDS) which requires appropriate data management and scheduling process. This paper proposed a Secure Scheduling Key Management Deep Learning (SSKMDL) for the e-commerce in healthcare application. The SSKMDL model uses the key authority quantum channel for the key generation to minimize the eavesdropping, transmission error and data leakage to increase the security. The E-commerce user and content server communicate key server with the quantum channel for the encryption key and key server for the public channel in the groups. The SSKMDL models evaluate the different generated secret key for the user quantum distribution key to increase security with appropriate data management. Additionally, the SSKMDL model uses the nature-inspired algorithm for the accurate scheduling and detection of attacks in the data. The deep learning E-commerce application increases the detection rate of intrusion with the hybrid effectively and efficiently for the classification of anomalies network traffic and hybrid regression and Decision Tree model. The performance of proposed SSKMDL model is evaluated for the Network Security Laboratory Knowledge Discovery in Data Bases (NSL KDD) dataset and real-time E-healthcare dataset. The analysis stated that SSKMDL E-commerce model exhibits the optimal group key for the training and testing to achieve efficient data management with scheduling to increase security. The experimental results expressed that proposed SSKMDL model utilizes deep learning model for the generation of key, optimization, healthcare encryption and decryption to increase the security with deep learning model. With constructed SSKMDL model eavesdropping rate is reduced by 80% with the increases attack detection rate of 99%.

Keywords: E-Healthcare, Data Security, Intrusion Detection System (IDS), Deep Learning, Scheduling, e-commerce

1.Introduction

E-commerce, short for electronic commerce, refers to the buying and selling of goods and services over the internet [1]. This can include everything from online retail stores and marketplaces to digital downloads and online bookings for services such as travel or healthcare. E-commerce has become increasingly popular in recent years [2], as more and more people turn

This is an open access article under the CC BY-NC license (https://creativecommons.org/licenses/by-nc/4.0 /)

to the internet to shop and conduct business. Some of the benefits of e-commerce include [3]: Convenience, Lower costs, Greater selection and Personalization. E-commerce has also created new opportunities for businesses, particularly small and medium-sized enterprises (SMEs), to reach a wider audience and expand their customer base beyond their local region [4]. Also, E-commerce subjected to different challenges of security, payment and prevention of fraud, customer trust, Logistics Management, Legal and Regulatory Compliance and Technological advancement [5 – 8]. Among those, Security is a major concern in e-commerce due to the sensitive nature of transactions and the potential for cyber-attacks [9]. E-commerce platforms are vulnerable to various forms of cyber threats, such as hacking, phishing, and malware attacks. These attacks can result in data breaches, identity theft, and financial loss [10]. Ensuring the security of online transactions and protecting customer data is crucial to building trust and confidence in e-commerce platforms with increase in number of users [11].

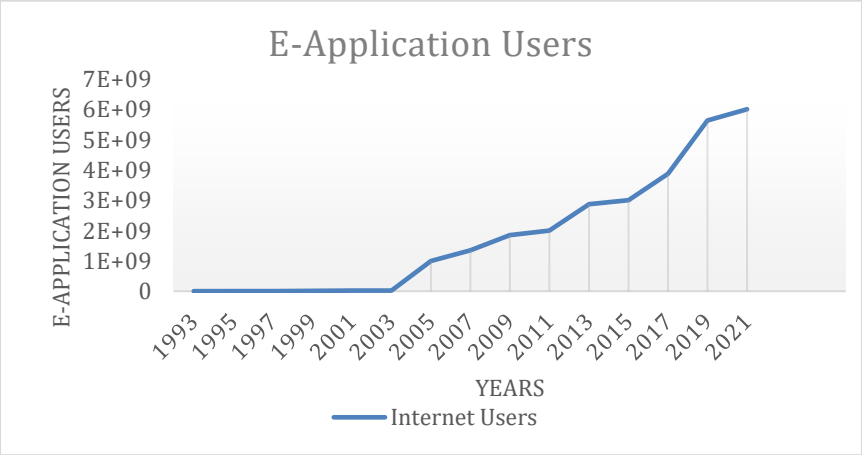


Figure 1: Exponential Growth in E- Commerce Application Worldwide (Source: http://www.internetlivestats,com)

The Figure 1 depicts a graphical view of the explosion in growth of the E-application since 1993 to 2021. It shows that growth is about to reach 3.5 billion users (individuals who can access the Internet at their home, using any device type and connection) worldwide in a short span of three decades [12]. In December 1995, the Internet was populated with 16 million users, which accounts to 0.4% of the world population [13]. By December 2015, it grew to 1018 million E-application users, which constitutes 15.7% of the world population. In March 2017 a record growth of 3,793 million users, 49.6% of the world population was witnessed as per the Internet world statistics (Source: www.internetworldstats.com) individuals, commercial organizations and government have loaded the E-Commerce with abundant amount of real-time, sensitive data and many mission-critical applications [14].

An Intrusion Detection System (IDS) is an important security tool that can play a critical role in protecting E-commerce platforms from cyber-attacks. The role of IDS on E-commerce platforms can be the detection of a network attack, application attack, user behaviour monitoring, alert generation, and examination of attack patterns. The performance is effectively management and processed with the implementation of the effective data management process. Intrusion detection perform the estimation of attacks in the networked computing for the causing harm or compromise in the intrusion in terms of Confidentiality, Integrity and Availability (CIA) [15]. Intrusion detection system subjected to different attacks against the vulnerability for the services, privilege of the users in hosts or implementation of malware and so on. Intrusion detection

system provides the non-compliance information system or attacks for the detection for the network facility computing. IDS is the automated tool for the design and implementation of the hardware or software combination utilized for the detection [16]. The IDS scheme is most effective security technology for the provision of different mechanism for the enterprises networks. As the IDS system is considered as the handy tool for the security or burglar alarm for the configuration of log events, utilized for the forensic punish adversary [17]. Conventionally, the IDS system triggers the higher rate or false alarm to eliminate the hindrance. An IDS provides visibility and control which are the two key aspects that aid in securing a network. Visibility makes the network traffic apparent helps in decision making thus influencing in security policy building directly. Control, in turn, is used to prohibit access to privileged areas in computer networks, which is otherwise used to impose compliance to the security policy [18].

A review of the best-known IDS from literature has helped us identify the high priority issues that are to be addressed. Proactive and accurate detection of intrusion in real time enterprise computer network continues to be a big challenge for automatic IDS [19]. The operation and uptime of the network is affected when there is an improper operation of the IDS, when certain attacks go undetected. Such security incidents results in heavy losses both to the enterprises and to the nation at large [20]. The performance of the IDS has not been effective due to ambiguity that prevails in detecting anomalous network traffic. It is very difficult to predict the difference or to clearly identify the difference between normal and anomalous network traffic. The most important showstoppers in the performance of automatic IDS are as follows [21] Classification of the mistrustful packets Classification refers to the detection of intrusive network traffic. Network traffic is busty and most times, the hostile packets are camouflaged with the benign packets Ambiguity Management Due to a certain degree of vagueness that exists in the periphery between normal and anomalous network traffic, it is very difficult to classify the network packets in a reliable manner [22]. Therefore, optimally classifying intrusions in a network flow continues to be a challenging task. An inference engine is to be trained with precise and latest knowledge in order to handle and classify the audit data in a robust manner in high-speed production networks. Hence, deep learning model are observed as the effective model for the attack classification and detection in the IDS system.

E-healthcare, on the other hand, refers to the delivery of healthcare services and information through electronic means, such as the internet, mobile devices, and telemedicine. This can include everything from virtual doctor consultations and remote monitoring of patients to online health education and self-diagnosis tools. E-commerce can be used to sell healthcare-related products, such as medical devices, supplements, and health foods, used to facilitate online appointments and consultations with healthcare providers, used to purchase and deliver medications, making it easier for patients to access the medications they need and used to sell healthcare services, such as virtual physical therapy sessions or mental health counselling. With the implementation of E-commerce in E-healthcare application to provide patients with easier access to healthcare products and services, as well as more convenient ways to manage their health.

This paper developed the SSKMDL model for the efficient data management and scheduling in the E-commerce business with the use of Intrusion Detection System (IDS) to increase security. The proposed SSKMDL model performs the cryptographic process and classification process for attack detection and anomaly detection in the network. The constructed

SSKMDL model uses the quantum channel for the estimation of the users in the network for the balancing load in the network to management and process the e-commerce data. The SSKMDL model generates the keys for the security in the e-healthcare data. The attributes of the e-commerce data stored in cloud about patient demographic information, health condition, diagnosis, insurance, medicines and so on. Those are encrypted with the generated key and stores in the cloud. With the generated key the IDS is implemented with the deep learning model for the attack detection and classification. The SSKMDL model performance is evaluated for the NSL-KDD dataset to train the model about the attack in the network of the attack detection in IDS. To evaluate the performance of the proposed SSKMDL in real-time dataset e-healthcare information are utilized and evaluated for the attack detection. Simulation analysis expressed that proposed SSKMDL achieves the 80% improved attack detection rate than the conventional techniques.

The paper is presented in total 5 sections: Where Section 1 presented the generic background information about the attacks in the network. Section 2 provides the background information about the existing literature on the attack detection and classification. Section 3 provides the detailed description of SSKMDL model with the dataset attributed utilized for the training and testing in deep learning model. Section 4 presented the simulation analysis of the SSKMDL model performance for the attack detection, key generation and classification is presented with the overall conclusion presented in Section 5.

2.SSKMDL Automated IDS

Automatic Network Intrusion Detection System (ANIDS) is a security tool used to deter corporate and military network intrusions along with other security tools. It is an essential second line security protection mechanism used by administrators and security personnel in order to implement certain required security policies. The existing state of the Internet system, the cause, and the financial after-effects of cyber security incidents, need for an IDS. Intrusion Detection (ID) is a continuous process involved in detecting inapt, wrong or anomalous action (break-ins, penetrations and any other forms of computer abuse) attempted by intruders or legitimate users of the ICT facility. An Intrusion Detection System (IDS) is a software tool installed in a dedicated, special purpose hardware device used to monitor the network or system activity under vigil and subsequently to generate reports to a management station or console.ID Process involves the following three steps as shown in the Figure 2. Monitoring and capturing the audit data, Analysing the audit data and detecting for the presence of anomaly and assessing the severity of the anomaly, raising alarm and taking corrective action.

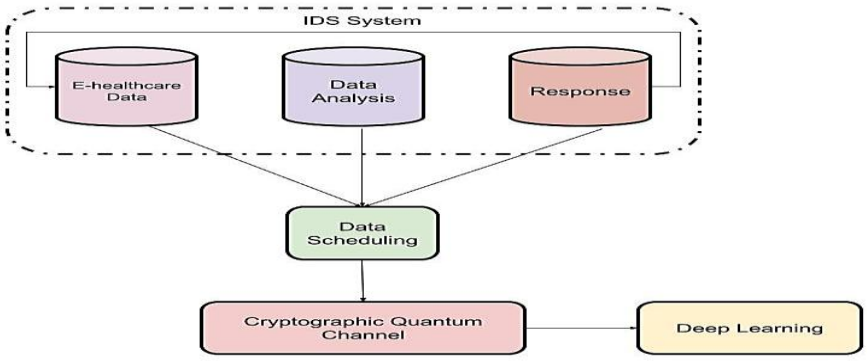


Figure 2: Steps in SSKMDL

2.1 Deep Learning Master-Key Management

The developed Secure Scheduling Key Management Deep Learning (SSKMDL) comprises of two modules as Generation of Key and encryption module with the implementation of the master key generation for the E-commerce business. The proposed SSKMDL model performs the communication within the group for the secure group with master key available within the intruders. The SSKMDL model comprises of the prime number such as $\boldsymbol{X_i}$ and $\boldsymbol{Y_i}$ with the master key. The prime number comprises of the $2 * primenumber + 1$. With the uses of $\boldsymbol{X_i}$ and $\boldsymbol{Y_i}$ public master key is determined easier represented as $\boldsymbol{e_i}$. Among the users the generated keys are generated and encrypted between the distributed users. However, the all users are performed to share the keys between users. The group of authorized users provides the access for the generated key. With the key request keys are distributed for the encryption of generator Group key for the healthcare data for the patient information in healthcare sector as $\boldsymbol{E_k}$ for the server content and data decryption for the healthcare users $\boldsymbol{D_k}$ for multi-group communication. The parameter values for the SSKMDL estimated as follows in equation (1) – equation (9):

$$\boldsymbol{A_i = (x_i - 1)/2} \quad (1)$$

$$\boldsymbol{B_i = (y_i - 1)/2} \quad (2)$$

$$\boldsymbol{e_i = 4 * Random + 1} \quad (3)$$

$$\boldsymbol{D_i = e_i^{2(A_i-1)(B_i-1) mod\ 4(A_i*B_i)}} \quad (4)$$

$$\boldsymbol{n = n * (A_i * B_i)} \quad (5)$$

$$\boldsymbol{L[i] = \frac{n}{A_i * B_i}} \quad (6)$$

$$\boldsymbol{M[i] = L[i]^{(A_i-1)(B_i-1)-1 mod\ (A_i*B_i)}} \quad (7)$$

$$\boldsymbol{e_{mas} = 0\ at\ initially} \quad (8)$$

$$\boldsymbol{e_{mas} = e_{mas} + (e_i * L[i] * M[i]) mod\ n} \quad (9)$$

The key management scheme comprises of the SSKMDL model for the healthcare data security for the data security with the deep learning. The secure deep learning model compute the multi-key in the server application for the estimation of healthcare data.

The model SSKMDL performs the identification of the local hosts for each server $\boldsymbol{U_{max} = 20}$. Here, the susers' servers are computed for the healthcare data for the automated allocation of the healthcare data in the next server. In the Server 1 the users within the 1 to 20 are incorporated within the local host of 8182 for the users directed with the identification of users in the local host 8236. Similarly, for the dynamic users the severs are balanced with dynamic loads with the merging with other servers in the minimal number of users. With SSKMDL model all servers comprises of the enrolled servers and patients for the medical healthcare system stated as Medical Service Registration Centre (MSRC). The procedure for the registration with the SSKMDL denoted in figure 2 and Process of Registration in E-Commerce in Figure 3.

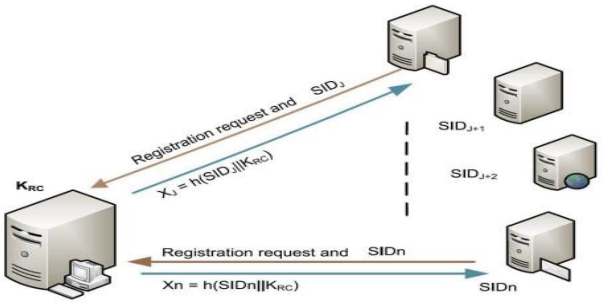


Figure 3: Process of Registration in E-Commerce

In proposed SSKMDL model all servers perform the registration process with the MSRC model stated as $(MS_j, j = 1\ to\ (m + m_0))$. In the developed model the servers m are registered for the medical servers. The medical servers comprise of the unique id with the SID_j transmission with MSRC for the registration phase. The MSRC registration centre server specific key value of $X_j = h(SID_j|KRC)$, where KRC comprises of the secret key with $MSRC$. The same process model $MSRC$ for the total process registration server as m number. In similar manner, $MSRC$ assume the server m' number for the registration process. The $MSRC$comprises of the unique server id denoted as SID_k for $m + 1 \leq k \leq m + m'$ and shared key value X_k for $m + 1 \leq k \leq m + m'$.The server ids and corresponding keys stored databased value of MSRC model for the server registration of requests for the unused unique id and corresponding database keys.

2.1.1 E-Healthcare Optimization Network Design

Proposed SSKMDL Group key algorithm

Step 1: Key Agreement in Pairwise Operation

Training process for the pairwise key generation

node pair (i,j) =pairwise key k(i,j)

for (i,j) € {(1,2),(2,3),(3,1)}.

Step 2: Key Agreement

Based on independent segment pairwise keys are divided.

$K_{3,1}$=($K_{3,1}^3$, $K_{3,11}$) , $K_{1,2}$=($K_{1,21}$, $K_{1,22}$), $K_{2,3}$ =($K_{2,32}$,$K_{2,33}$).

Node 1 broadcasts $K_{1,21}$ $K_{3,11}$, so node 1 and 2 obtain both $K_{1,21}$ and $K_{3,11}$

SSKMDL Group Key Generation for the E-commerce data

Step 1: Pair-wise Agreement in the Key

With the deep learning-based training process pair-wise keys are generated for the nodes M and 1 with pair-key of K_1 and nodes are in the range of -1 and m with pair-wise key denoted as $K = 1, 2, \ldots\ldots, M$.

Step 2: Key Agreement

In each independent segments pair-wise keys are divided as the M-1 with generated group key for node m for the random key $k^{|m|}$ generated. With the next node encryption is performed in the next node$m$ + 1 when m<M, or node 1 when m=M for pair-wise segment of $K_m + 1$ for node 1 when $m = M$ for encryption process $K_m + 1$. The generation of the key is evaluated based on the number of nodes M-1 for node M. The group *M* nodes are estimated as $K|1|, K|2|, \ldots\ldots\ldots, K|M|$ for group key. The final group key generation is evaluated for the computational cost with the encryption of e-commerce data through quantum key.

2.2 Deep Learning SSKMDL Attack Detection Model for E-healthcare

An algorithm on the clustering behaviour of lives is stated as genetic algorithm. By nature, self-organized work as a team to group similar objects in clusters. In the algorithms modelled for clustering, ants and objects are modelled as basic entities. Each object represented as Om has its own feature represented as f_{mn}. The objects to be clustered in the problem space are represented as j-dimensional vectors as in equation (10) and equation (11)

$$\{O_1, O_2, \ldots\ldots, O_N\} \quad (10)$$

$$O_m = \{f_{m1}, f_{m2}, f_{m3}, \ldots\ldots, f_{ml}\},\ m = 1,2,3, \ldots\ldots, N \quad (11)$$

Where N refers to object count and j refers to the dimension of features. When applying GA to the network intrusion detection domain, each network traffic record having their own

features is viewed as objects. These objects can be clustered into normal or an abnormal class based on the values the features hold.

Algorithm 1: intrusion detection by SSKMDL
Input: SSKMDL -GA classifiers Input: New audit data record a Output: Detected class label – C 1. Begin 2. Classification of a by OSVM – C_s 3. Classification of a by DAC – C_A 4. If $C_s = C_A = normal\ then$ 5. C = Normal 6. else if $C_s <> C_A$ then 7. C = ambiguous 8. Else 9. $C = C_A$// subclass assignment of anomaly 10. End

The detection process is a hybrid approach by combining regression and decision tree. The input to this algorithm is a record from the audit dataset and the combination of regression and decision tree. The classification is based on the consideration of the e-commerce data. The DAC further classifies the attack class to particular type of the attack. The classification of the audit record into either one of the five classes is the output.

2.3 NSL KDD Dataset Descriptions

A collection of dataset (KDD99, Kyoto, Australian Defence Force Academy Linux Dataset (ADF-LD), etc.), are available for the research community to evaluate their proposal, but they rarely simulate the real time network traffic. As the developed model focused on the E-commerce data for the E-healthcare application analysis is performed with the NSL-KDD based software engineering model is utilized. Whereas the NSL KDD dataset is refined, unbiased and contains lesser records than its predecessor, the KDDcup99 dataset. Hence this dataset has been used in this study for various evaluation purposes. A benchmark dataset is already pre-processed and contains records representing all possible real time network traffic. The size of the dataset is reasonable, and the complete dataset is used for evaluating the NIDS, which proves the consistency, validity and reliability of the results obtained. The features available in this dataset are either numerical (continuous) or nominal (discrete). The various dataset files available for evaluation of the NIDS along with their description is given in Table 1. (Source: http://www.unb.ca/cic/research/ datasets/nsl.html).

Table 1: NSL KDD files and description

File Name	**Description**
KDDTrain+.ARFF	The files in ARFF comprises of the binary labels for the NSL-KDD training set.
KDDTrain+.TXT	The file comprises of the labels for attack-type for the NSL-KDD train with the difficulty level of CSV format.
KDDTrain+_20Percent.ARFF	KDDTrain+.arff file comprises of the subset of 20%
KDDTest+.ARFF	The ARFF formatwith the test set of NSL-KDD for the assigned binary labels

KDDTrain+_20Percent.TXT	A 20% subset of the KDDTrain+.txt file
KDDTest+.TXT	With NSL-KDD dataset comprises of the CSV format for the testing data with the assigned attack labels.
KDDTest-21.ARFF	A subset does not comprise of the records for the KDDTest+.arff with complexity level of 21 out of 21.
KDDTest-21.TXT	A KDDTest+.txt subset does not incorporate records complexity of 21 out of 21.

The selected dataset comprises of the features 41 and attribute with 1 class for the 21 categorized attacks in 4 classes such as Probe, User to Root (U2R), Remote to local (R2L) and the Denial of Service (DoS). The 3 different groups comprise of the 41 features with basic, content and traffic. The basic features are extracted from the TCP/IP connection and these features are very important to detect many attacks. Content features of the dataset help in the detecting suspicious traffic, whose traits are hidden in the payload of a network packet; these features are of high importance in detecting R2L and U2R attacks. Traffic features are further classified as same host feature and same service feature, whose value is based on the connection established in the past 2 seconds. The total number of records, distribution of records of various classes and their percentage is given in the Table 2.

Table 2: NSL-KDD dataset classes

Dataset Type	**Number of records**					
	Total	**Normal Class**	**DoS Class**	**Probe Class**	**U2R Class**	**R2L Class**
KDD Train+ 20%	26882	146826	9147	2479	19	213
		55.25 %	38.36%	10.03%	0.03%	0.94%
KDD Train+	165735	68644	46793	13472	59	978
		54.77%	38.46%	9.33%	0.03%	0.83%
KDD Test+	23567	9846	7368	2368	215	2964
		45.68%	36.57%	11.36%	0.77%	11.36%

3.Results and Discussion

The SSKMDL perform implementation of the e-commerce data security in terms of genomic sharing, exchange of health information, cloud Network, Offices & clinics, Insurance, Hospitals, Telemedical Network, Healthcare Network and so on those are dynamically joined and leaving the network. With guaranteed multicast domain capacity is performed for the transmission and handling time in scheduling servers. The time taken for the E-commerce user for the variation in the time for the different levels. Initially, the first trees comprise of the two users and observed for the time taken for communication for the one and two users in the different E-commerce data. The generated master key with the utilization of public key pairs is presented in table 3.

Table 3: Master key generation

Parameters	Quantum Key – Channel 1	Quantum Key – Channel 2
Xi	5, 7	5, 7, 11
Yi	23, 47	23, 47, 59

Ai	2, 3	2, 3, 5
Bi	11, 23	11, 23, 29
ei	92177, 46133	37663, 2064, 99869
Di	73, 17	29, 5, 149
L[i]	15, 18	220110
M[i]	69, 22	10005, 3190, 1518
n	39, 160	12, 220, 32
e_{mas}	2549	129209

With the two-level tree model group are computed for the users 4 for the varies time taken with user addition with one by one in the 4 users. The 2-level tree generation is computed for the variation in the time. The variation in number of users, message size, no changes in difference in time. With the increased number of users, the variation in time is estimated for the 3-level tree analysis for the effective changes in time for the number of user's increases for the 8 users. The relation between the SSKMDL keys is estimated for the authentication process to perform key authority for the slave key estimation in the user groups is presented in table 4.

Table 4: Key Management with SSKMDL

Users (N)	E-commerce data (kB)	Time (sec)	Smoothing constant (k=N/T)
5	5	9	0.23
10	25	11	0.37
15	25	13	0.39
20	30	16	0.375
25	30	27	0.27
30	30	93	0.093
35	35	158	0.07

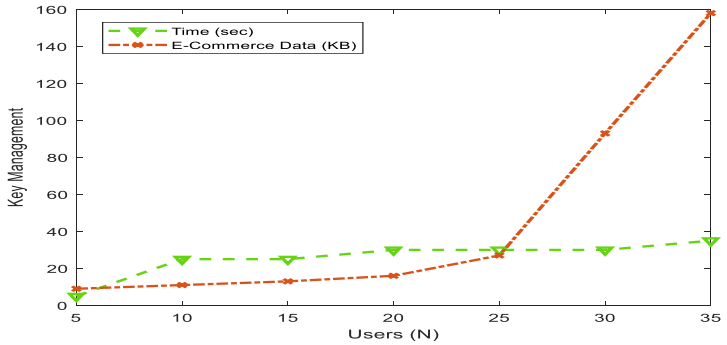


Figure 4: Scheduling with the E-Commerce data

The analysis of completeness of sample electronics patient records was presented in figure 4 for the scheduling process. Also from Table 5, the importance of electronic health record data completeness and how different conceptualizations of completeness may impact findings from various patient data was demonstrated.

Table 5: Analysis of E-Commerce Data

Data	**Fraction of Patient Features**	**Average E-commerce data documented**	**Average data completeness (C=A×B)**

Demographic Profile of Patients	0.89	0.92	0.81
Age	0.91	0.93	0.87
Characteristic of Patinets	0.38	0.82	0.31
Education	0.37	0.19	0.08
Sex	0.97	0.91	0.90
Health status	0.67	0.79	0.51
Symptoms	0.88	0.82	0.71
Pregnancy	0.33	0.53	0.17
Disease stage	0.34	0.53	0.18
Allergy	0.29	0.73	0.21
Organ Conditions	0.72	0.82	0.59
Lifestyle	0.83	0.86	0.71
Addiction	0.73	0.76	0.53
Diagnostic test	0.59	0.39	0.23
Lab results	0.59	0.41	0.23
Treatment	0.59	0.48	0.29
Medication	0.38	0.23	0.09
Therapy or Surgery	0.76	0.49	0.38
Ethical concern	0.09	0.77	0.08
Consent	0.09	0.53	0.04
Capacity	0.18	0.79	0.16

The key generation scheme is implemented in the JAVA with examination of the public parameter's initialization, generation of key, derivation in group key, encryption time and decryption time computation time. The SSKMDL model uses the management of ElGamal group key, fast Chinese, key schemes for the computational cost for the encryption and decryption process. In table 6 effectiveness of the proposed SSKMDL key generation method by measured computation time in milliseconds for conventional method with key generation process.

The figure 5 provides the key management scheme comparative analysis with the proposed SSKMDL model. The e-commerce security model performs the verification in login and encryption of data. The file in login is connected to the specified users to perform the information exchange about the patient and increased liability. The comparative analysis stated that increase in group size the server key is multiplied in virtual key server to perform the faster e-commerce data to increases the security and sensitive communication information transmission. The developed SSKMDL model performs the group key management with the reduced threats as much as possible compared with the existing techniques.

Table 6: Key Management with SSKMDL for the computational complexity

Scheme	**ElGamal**	**Fast Chinese remainder**	**SSKMDL**
Group key	78	105	15

Public key	196	148	86
Encryption	359	489	214
Decryption	968	690	186
computational cost in ms	1782	2698	845

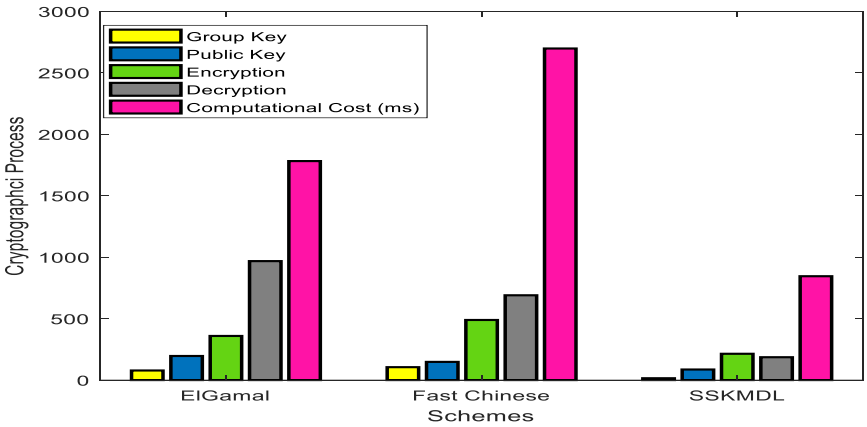


Figure 5: Comparison of Key Management

3.1 Experimental results for the NSL KDD dataset

This section discusses exhaustively about the results produced by the SSKMDL when evaluated with the benchmark NSL KDD data set.

Table 7: Precision of the training data

Class	**Precision (%)**	**Recall (%)**	**F-measure (%)**	**Accuracy (%)**
Normal	99.07	98.79	97.41	97.30
DoS	98.36	97.40	98.55	98.61
Probe	94.56	98.46	99.24	98.91
R2L	96.82	97.62	96.35	94.56
U2R	97.46	95.36	94.26	97.63

The precision percentage obtained by the SSKMDL for various classes of attacks is shown in table 7. The precision values for Normal, DoS, Probe, R2L and U2R classes are 96.07%, 98.70%, 98.03%, 98.56% and 98.97% respectively.

Table 8: Precision of the testing dataset

Class	**Precision (%)**	**Recall (%)**	**F-measure (%)**	**Accuracy (%)**
Normal	97.40	98.39	97.87	97.95
DoS	98.62	98.47	98.54	98.65
Probe	97.56	99.35	97.56	98.72
R2L	98.34	97.36	98.24	99.25
U2R	97.56	96.25	97.25	97.63

Table 8 Comparison of testing dataset detection accuracy, precision, recall and F-measure of SSKMDL with the various other methods

Table 9: Comparative Analysis

Evaluation Metric	**[31]**	**[24]**	**[27]**	**SSKMDL (%)**
Accuracy	78.25	81.92	82.39	98.31
Recall	75.97	84.04	87.96	98.52
Precision	75.58	82.6	83.6	98.52

F-measure	78.72	83.31	85.72	98.25

In previous studies attained 88.10% in detection of the Probe attack, which is the second highest of all the other methods. The detection of R2L attacks stands 94.84%. The detection rate of R2L attacks by the other techniques listed in the Table 9 is comparatively lower. The detection rate of the infrequent U2R attacks by the SSKMDL is 98.58%, which is significantly higher than the other methods.

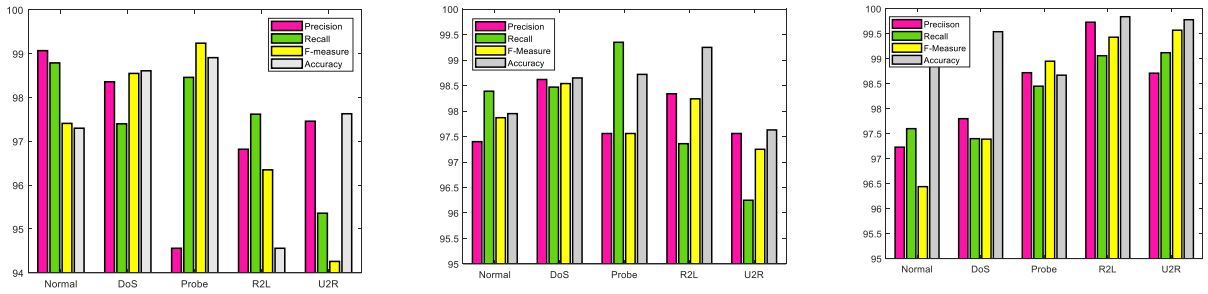
3.2 Experimental results for E-Commerce

This section discusses the experimental results produced by the SSKMDL when evaluated with the real time e-healthcare dataset utilized in E-commerce with attributes presented in table 10.

Table 10: SSKMDL with real time E-Commerce dataset

Class	Precision (%)	Recall (%)	F-measure (%)	Accuracy (%)
Normal	97.23	97.60	96.44	98.94
DoS	97.80	97.40	97.39	99.54
Probe	98.72	98.45	98.95	98.67
R2L	99.73	99.06	99.43	99.84
U2R	98.71	99.12	99.57	99.78

Table 10 shows the values for precision, recall, f-measure and accuracy of the SSKMDL for the real time data captured from the test bed. This data presented in the table is the average value of the performance measures of the train and test dataset corresponding. The figure 6(a) figure 6(b) presented the performance evaluation of the proposed SSKMDL model with the training and testing performance for the NSL-KDD dataset. The figure 6(c) presented the real-time healthcare dataset examination with the consideration of different attack classes in the e-commerce data.



(a) (b) (c)

Figure 6: Performance of SSKMDL for (a) NSL – KDD training (b) NSL – KDD testing (c)E-Commerce dataset

Table 11: Performance measures of E-Commerce

Parameters	Value (%)
Accuracy	99.25
Recall	98.35
Precision	96.98
F-measure	98.46

The evaluation parameters such as accuracy, recall, precision and F-measure are listed in

the Table 11. The accuracy is 99.25%, recall is 98.35%, precision is 96.98% and F-measure has recorded 98.46%. The SSKMDL intrusion detection method has comparatively produced better results for the real time data set.

4.Conclusion

E-commerce involved in buying and selling of good through Internet comprises of the online retail stores and marketplaces. Through E-commerce business users perform shopping with the use of Internet based on own convenience, low cost, selection and personalization. E-commerce is beneficial for the people with certain health issues for the receiving medicines, food, consultation and so on. However, due to the increase in effective utilization of patient information in E-healthcare need to be secure from the threats and attacks in the network. With the security scheme in E-commerce can be effectively utilized in the E-healthcare application for the medicine and other products to patients. To increase the security in E-commerce data SSKMDL model is implemented for the attack detection and classification through the IDS. The developed SSKMDL scheme uses the key management with the quantum channel for the management of key. With the generated keys load in the network are balanced for the attack detection and classification through deep learning model. The SSKMDL model performance is evaluated for the NSL-KDD and real-time e-commerce dataset. The attacks in the network are detected and classified based on the hybrid classification model with the regression and decision tree. The experimental analysis stated that SSKMDL model achieves the higher attack detection and classification rate of 99% which is significantly higher than the state-of-art methods. Through comparative analysis it is concluded that SSKMDL model is effective data management scheme with improved security in E-commerce application.

Acknowledgment: Not Applicable.
Funding Statement: The author(s) received no specific funding for this study.
Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] S. Vinoth, H. L.Vemula, B.Haralayya, P.Mamgain, M. F. Hasan et al., "Application of cloud computing in banking and e-commerce and related security threats," *Materials Today: Proceedings*, vol. 51, pp.2172-2175, 2022.
[2] S. Badotra and A. Sundas, "A systematic review on security of E-commerce systems," *International Journal of Applied Science and Engineering*, vol.18, no.2, pp.1-19, 2021.
[3] M.Zhang, L.Lin and Z. Chen, "Lightweight security scheme for data management in E-commerce platform using dynamic data management using blockchain model," *Cluster Computing*, pp.1-15, 2021.
[4] S. Luo and T. M.Choi, "E-commerce supply chains with considerations of cyber-security: Should governments play a role?," *Production and Operations Management*, vol.31, no.5, pp.2107-2126, 2022.
[5] R.Yu, C.Wu, B.Yan, B.Yu, X.Zhou et al., "Analysis of the impact of big data on e-commerce in cloud computing environment," *Complexity*, vol.2021, pp.1-12, 2021.
[6] Y. C. L. Tan, "Recent Technological Trends and Security Challenges in Trust-Building in E-Commerce," *International Journal of Business and Management*, vol.14, no.12, pp.226, 2021.
[7] Z.Dai and X. Guo, "Investigation of E-Commerce Security and Data Platform Based on the Era of Big Data of the Internet of Things," *Mobile Information Systems*, vol.2022, 2022.

[8] F. T.Abdul Hussien, A. M. S.Rahma and H. B. Abdul Wahab, "A secure environment using a new lightweight AES encryption algorithm for E-commerce websites," *Security and Communication Networks*, vol.2021, pp.1-15, 2021.
[9] F. T. A.Hussien, A. M. S.Rahma and H. B. A. Wahab, "Design and implement a new secure prototype structure of e-commerce system," *International Journal of Electrical and Computer Engineering*, vol.12, no.1, pp.560, 2022.
[10] Y.Yalan and T. Wei, "Deep logistic learning framework for E-commerce and supply chain management platform," *Arabian Journal for Science and Engineering*, pp.1-15, 2021.
[11] L.Li and J. Zhang, "Research and analysis of an enterprise E-commerce marketing system under the big data environment," *Journal of Organizational and End User Computing (JOEUC*), vol.33, no.6, pp.1-19, 2021.
[12] A.Toqeer, T.Alghamdi, A.Nadeem, Y.Perwej and M. Thabet, "Cyber security intelligence and ethereum blockchain technology for e-commerce," *International Journal*, vol.9, no.7, 2021.
[13] S.Vyas, S.Gupta, D.Bhargava and R. Boddu, "Fuzzy Logic System Implementation on the Performance Parameters of Health Data Management Frameworks," *Journal of Healthcare Engineering*, vol.2022, 2022.
[14] S. S.Kute, A. K.Tyagi and S. U. Aswathy, "Security, privacy and trust issues in internet of things and machine learning based e-healthcare," *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp.291-317, 2022.
[15] A.Kumar, A. K.Singh, I.Ahmad, P.Kumar Singh, P..K. Verma et al., "A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare," *Sensors*, vol.22, no.15, pp.5921, 2022.
[16] M. A. Kumaar, D. Samiayya, P.D. Vincent, K. Srinivasan, C.Y. Chang et al., "A hybrid framework for intrusion detection in healthcare systems using deep learning," *Frontiers in Public Health*, vol.9, 2021.
[17] M.Shamila, K.Vinuthna and A.K. Tyagi, "A review on several critical issues and challenges in IoT based e-healthcare system," *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, pp. 1036-1043, 2019.
[18] A.Kishor, C.Chakraborty and W.Jeberson, "A novel fog computing approach for minimization of latency in healthcare using machine learning," 2021.
[19] J.Lansky, S.Ali, M. Mohammadi, M.K. Majeed, S.H.T. Karim et al., "Deep learning-based intrusion detection systems: a systematic review," *IEEE Access*, vol.9, pp.101574-101599, 2021.
[20] J. P.Li, A.U.Haq, S. U.Din, J.Khan, A.Khan et al., "Heart disease identification method using machine learning classification in e-healthcare," *IEEE Access*, vol.8, pp.107562-107582, 2020.
[21] S. S.Kute, A. K.Tyagi and S. U. Aswathy, "Security, privacy and trust issues in internet of things and machine learning based e-healthcare," *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, pp.291-317, 2022.
[22] F.Akram, D.Liu, P.Zhao, N.Kryvinska, S. Abbas et al.,"Trustworthy intrusion detection in e-healthcare systems," *Frontiers in public health*, vol.1800, 2021.