VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2023, ISSN(e): 2309-3978, ISSN(p): 51-60
Volume 11, Number 1, January-March 2023 *pp: 51-60*

Secure Architecture for Electronic Commerce Applications Running over the Cloud

Mujeeb-ur-Rehman Jamali[1], Shahmurad Chandio[1], Nadeem Ahmed Kanasro[2]

[1]Institute of Mathematics and Computer Science, University of Sindh Jamshoro Pakistan
[2]Department of Computer Science, Sindh University Campus, Larkana, Pakistan
*Corresponding author email:mujeebjamali@usindh.edu.pk

ABSTRACT

E-commerce and mobile commerce are two new business methodologies that utilize the cloud. A new technology called cloud computing uses the Internet to process and store data from a network of distant computers that are dispersed around the globe. Any online transaction must have security as a necessary component. Therefore, one of the main issues with the cloud is security. If electronic commerce's security is breached, customers can lose trust in it. An unauthorized individual should not have access to or be able to intercept a customer's personal information while it is being transmitted. Data integrity is a major problem since personal information shouldn't be changed before, during, or even after it is at rest on the network. The suggested solution ensures the protection of personal data and the avoidance of security problems. We have developed a solution in this study to address issues with privacy, confidentiality, and the integrity of data stored in the cloud, among other security-related issues. The suggested method employs over-encryption that is double encryption, to avoid the various security issues. It can be inferred from the results that ECC (secp256r1) utilised less time for encryption operation as compared to others asymmetric algorithms with small dispersion from means and recorded results behaviour of data is consistent because data point tends to be very close, Decryption operation ElGamal during of time was smaller than ECC and RSA with small consistent behaviour.

KEYWORDS
Security, electronic commerce, cloud computing
JOURNAL INFO
HISTORY: Received: January 21, 2023 Accepted: March 10, 2023 Published: March 26, 2023

INTRODUCTION

Electronic commerce (e-commerce and m-commerce) offers non-cash payment options such as credit cards, debit cards, smart cards, electronic fund transfers through bank websites, and other electronic payment options with 24-hour service availability. It is automating businesses process and offer clients services. It is accessible everywhere and at all times. It broadens the audience for company marketing and promoting of their goods and services. It assists in better product/service marketing management. It increases sales since orders may be produced for the items at anytime, anyplace, and without the need for human participation. It significantly increases current sales volumes. It encourages and offers several options for pre and post-sale support to give clients better services. Additionally, it offers automated inventory control. When necessary, reports are immediately created. Management of the product inventory becomes incredibly effective and simple to maintain. It offers methods for quicker, more effective, and dependable communication with partners and consumers. There are main areas in which the benefits of internet commerce may be roughly divided. With a minimal financial commitment, businesses may expand their markets to include both domestic and foreign markets. Across the world, a firm may simply find additional clients, the best suppliers, and compatible business partners. Digitizing information aids firms in lowering the cost to produce, process, disseminate, retrieve, and manage paper-based information. It boosts the company's brand image. Better customer service is made possible by this for businesses. The business procedures are streamlined, which increases their speed and effectiveness. Paperwork is decreased by using electronic commerce. Customers may make inquiries about a good or service and place orders from any location at any time. Before making a final purchase, a consumer can post review remarks about a product, examine what others are buying, or read the review comments of other customers. As a result, businesses provide clients significant discounts. It fosters competitiveness among businesses. There have benefits for Society from it. It makes it possible for rural regions to get items and services that they would not otherwise have access to. Business-to-Business (B2B), business-to-consumer (B2C), consumer-to-consumer (C2C), and consumer-to-business (C2B) are the four broad categories for business models in electronic commerce. In a business-to-business transaction, a product is sold to an intermediary buyer who then sells it to the end client. Direct client sales are made under the B2C business model. The C2C business concept enables customers to sell their possessions, including homes, vehicles, motorbikes, and more. There are essentially two categories that may be used to categorize the drawbacks of m-commerce and e-commerce. A lack of system security, dependability, or standards may exist as a result of subpar implementation. Non-reputability is an issue in electronic commerce since it serves as a safeguard against the rejection of orders or payments. The security of personal data that is stored and sent over the Cloud is a major issue.

CLOUD COMPUTING

Cloud computing architecture enable huge, gigantic,

and cost-effective computing to run efficiently. Big Data workloads in cloud computing are easier to manage, easier to implement, and less expensive. Cloud hosting is a term used on the Internet to describe temporary on-demand access to resources such as storage, infrastructure, and applications. It is classified into three types: public, private, and heterogeneous of both, via which users may access services from anywhere and at any time. With the rise of the cloud, an application utilising an architecture that operates on a public and private cloud that supports Big Users and Big Data. Software as a service (SaaS) refers to the use of software rather than its purchase. The platform service (IaaS) environment allows users to create/develop and run applications. Infrastructure as a service (IaaS) provides on-demand computer power and physical capacity, such as storage and space [1].

Insider attackers in the attack model include database administrators, employees, ex-employees, and contractual staff who may be malicious and curious because they know about the user's data and can easily gain access to useful data, sensitive and confidential information, posing a threat to data confidentiality, integrity, and authentication. Insiders have varying levels of access to the data housed in a document database. Deliberate malevolent insiders may eavesdrop and steal data for a variety of nefarious motives, which may end up in the wrong hands. In this instance, the database server should not be trusted since a hostile administrator may obtain access to valuable data. The issue with data at rest encryption is that insiders may access the encrypted data since they know the secret key used for ciphertext decoding. The attacker is neither a database user nor a database administrator in an external and outside attack. Unauthorized access and dissemination of information from outside sources.

PROBLEM STATEMENT

Problems and difficulties with security in applications for electronic commerce included data tampering, information leakage, eavesdropping, man-in-the-middle attacks are some of the security challenges that cloud computing faces.

DATA TAMPERING

A significant worry with cloud-based data is data tampering. Due to flaws, it's possible for an ill-intentioned insider or outsider to access and change data at a cloud service provider. It is crucial to confirm that it is original and unaltered from when the user sent it. It is the user's responsibility to check and confirm any changes made to any cloud-based data that they have stored. Data integrity can be verified using an asymmetric cryptographic algorithm.

EAVESDROPPING

It is possible for an unauthorized user or attacker to eavesdrop on data being transmitted between a sender and a receiver. An unauthorized user may steal or covertly reveal sensitive information during an eavesdropping attack.. Eavesdroppers who employ a passive attack can read data without interfering with the system's regular operation. During a data at motion attack, unencrypted or sensitive data is tracked and analyzed. Passive attacks cause sensitive or confidential data to be revealed to an attacker without user knowledge or consent. Data content is observed in this kind of attack without permission (seek explicitly). Because only the intended user can read, passive attacks pose a threat to confidentiality. The user may not be aware of the attack, which is more severe, and the system is unaffected or not harmed. Using an asymmetric cryptographic algorithm can prevent this attack. Encryption is used to reduce the risk of malicious practices using private/confidential data and other useful information without permission.

MAN IN THE MIDDLE ATTACK

The most dangerous type of attack, known as a "Man-in-the-Middle," involves an intruder connecting to the sender and receiver in order to intercept data transmission. The attacker in this attack intercepts either the secret key or the public key. The data sent by the user can then be read by the attacker. For the purpose of preserving communication between the parties, the ciphertext is produced using the secret or private key. Since transaction level security is also provided by the Secure Socket Layer, all system components were able to successfully communicate with one another in a secure manner.

RELATED LITERATURE

For e-commerce and m-commerce apps, there are a variety of security problems and vulnerabilities. Some threats and security issues regarding applications are mentioned that in cloud computing, data are kept on distant servers and the user is unaware of the location of the data, raising concerns about malicious data modification, or illegal modifications made to persistent data. Data integrity must be offered so users can verify that data has not been tampered with, compromised, or altered [1][2][3]. Private and confidential information disclosure threats in cloud computing involve exposing information to people who shouldn't have access to it, such as users' ability to read a file to which they weren't granted access or an intruder's ability to read data while it's being transferred between two computers. Strong encryption, key management, and authentication may be utilized to prevent such security risks [3]. When data is sent between senders and receivers in the cloud, it is conceivable for an unauthorized user to eavesdrop on the communication. To reduce the possibility of such a risk, encryption is frequently employed [4]. In eavesdropping attacks, unauthorized users may steal or covertly divulge personal information, including public and private keys, digital certificates, and other important information.

In [5] empirical study was carried out using secret key algorithms such as AES, DES, and Blowfish. The execution performance of the following algorithms was compared based on CPU time. There are two (2) datasets used: small and huge. File sizes for small and big datasets range from 100 bytes to 1000 bytes and 10,000 bytes to 100,000 bytes, respectively. The author(s) discovered that the average execution time in

milliseconds on small data text files was 198.5 (AES), 184.4 (DES), and 185.1 (DES) (Blowfish). Based on actual results of time limitations, the author (s) discovered that AES took 8% less time / slower than DES, and similarly AES took 7% less time / slower than Blowfish. As a result, for small dataset encryption, DES was quicker than both techniques. Meanwhile, for big datasets, three techniques required almost the same time to encrypt and decrypt. In terms of memory constraints, it was discovered that DES was 1.01% slower than Blowfish but used 0.63% less memory to execute the AES algorithm. AES took 2.48% more memory than Blowfish for big datasets, and 1.34% more RAM than DES. As a result, Blowfish outperformed other symmetric algorithms. Algorithms are used in financial applications such as the stock market and e-commerce.

The authors of [6] gave a performance evaluation of the ElGamal, RSA, and ECC key pair generation algorithms. Table 1 shows the millisecond plaintext transformation of 159 bits encryption with public key and decryption with private key. The result suggested that ECC had an edge over RSA and ELGamal in encryption. The authors proposed that in future work, data compression on the encrypted plaintext be used to reduce the amount of the ciphertext.

Table 1: ElGamal, RSA and Elliptic Curve Cryptography

Key size	RSA	ElGamal	Elliptic
Key Pair Generations			
160	951	406	2437
256	1957	895	6451
512	16863	15946	40317
1024	76498	68773	318574
Encryption with Public Key			
160	18	2816	2696
256	37	7098	8242
512	258	29388	57236
1024	2013	140979	411558
Decryption with Private Key			
160	10	18	1292
256	37	37	3932
512	259	194	27034
1024	1966	1107	198823

In [7] based on PKI and the owner-write user-read scenario, Owner, user, and SSP are the three participants in the system. In this arrangement, the owner encrypts all the data using a secret key and uploads it to the SSP for privacy. In this architecture, the secret key is shared between the owner and all users while being kept a secret from the SSP to ensure the privacy of the outsourced data. The Access Control Metric (ACM) for the outsourced data is created by the owner during this procedure, and the owner also produces its signature. The owner then delivers the ACM and its signature to the SSP. For over-encryption, SSP selects a random session key in the meanwhile. Before transferring the data to the user, SSP encrypts it with a one-time session key; however, the session key is then encrypted once more using the public key of the authorized user. Here, the encrypted session key can only be decrypted and used to access the data by the authorized user. Therefore, no one who is not allowed may access the data (Figure 1).

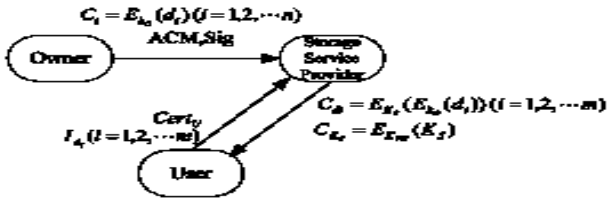

Figure 1: owner-write-user-read PKI model

Three participants—DO, User, and SSP—contributed to the work in [8]. Due to the lack of confidence in SSP, DO encrypts data before storing it there, and in order to obtain data that is safe and efficient, access systems employ a special combination of encryption and capability-based access control. In this system, the user is given keys and a digital certificate. SSP receives a digital certificate from the user, and if it is genuine, SSP sends the user encrypted data. The capability list and encrypted data in this system are supplied by DO. SSP, on the other hand, uses its own private key as well as the DO's public key to decrypt the message and store the encrypted contents and capability list in its storage. Because the secret key is shared by the user and the DO in this architecture, the SSP is only able to decode the data; they cannot read it. The system's biggest drawback is that DO is constantly online and that it encrypts data before storing it in SSP (Figure 2).

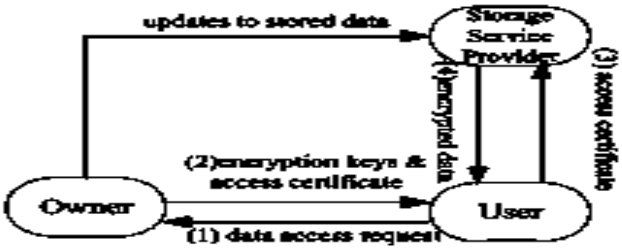

Figure 2: Cryptographic model

METHODOLOGY

The research was conducted using empirical techniques and frameworks. Issues have been examined and addressed using quantitative data that has been gathered. Adoption of contemporary asymmetric cryptography. The most crucial tool for safeguarding sensitive and private data is the proposed methodology's use of asymmetric algorithms, which offers security.

RESEARCH DESIGN

The research design serves as a framework for organizing the overall work of research. It serves as the theoretical groundwork for the investigation. Since it ties the entire research work together, it is crucial. To provide for the gathering of relevant data is its main goal (shown in Figure.3).

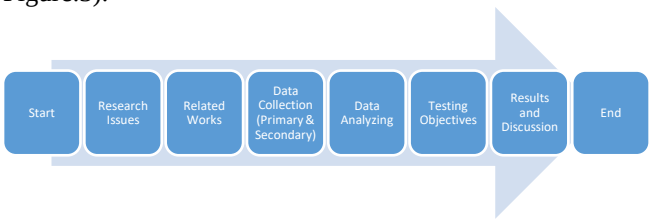

Figure 3: Design Process

DATA COLLECTION

There are various methods and techniques for gathering the correct data, and there are different ways to do so. the sources used to gather information for the study. Data collection involved the use of primary and secondary sources. In empirical research, which is the first-ever data collection in quantitative format, the primary data is directly gathered by the experiment. The secondary data is information that has already been gathered or acquired by other researchers and makes data found in periodicals and other published sources available.

DATA ANALYSIS

The research's findings are ascertained through analysis of the collected data using the accepted method for presentation. Additionally, a tabular format is used to display the frequency's summarised mean, percentage, and standard deviation, with the same to be discussed in more detail in the results and discussions sections.

SOLUTION DEVELOPMENT

The proposed system was implemented using Java and the Windows operating system, and a working prototype of the system has been produced. The three main categories are Small, Medium, and Large datasets. For key pair generation, encryption, and decryption, an asymmetric algorithm is used. quantitative outcomes from the generated empirical data by our system. In the results and discussion sections, a statistically sound analysis of the results that were founded is presented in detail.

EVALUATION

Asymmetric algorithms are used to safeguard data while it is at rest. Pair of keys are generated. To encrypt data and protect it. Private key is used to convert the ciphertext back into plain text.. The public key is applied to encryption. Longer-sized keys are used for greater data protection.

Security at the transaction level is also provided by the Secure Socket Layer (SSL). SSL provides end-to-end privacy, integrity, and authenticity for the protection of data in motion. At both the sending and receiving ends, this offers transaction level security. The system was developed and put into use for data synthesis. For the purpose of gathering accurate data, each operation was carried out atleast ten times. The analysis of the result synthesis was then carried out.

LIMITATIONS

A limitation of asymmetric cryptography is that medium datasets (i.e. 276 bytes) of plaintext cannot be encrypted using a ElGamal key size of 256 bits. Additionally, the RSA algorithm has a maximum key size (i.e. 4096 bits) of can be used encryption and decryption of medium-sized dataset, Both ElGamal (256) and RSA (4096) algorithms are unable to complete the encryption operation on large dataset of 529 bytes of plaintext.

The practical ElGamal algorithm's limitation prevents it from supporting data sizes larger than 16 bytes with 128-bit public and private keys. With 192 and 256 bits of the key, it can encrypt 23 bytes of plaintext.

For plaintext encryption and decryption, the RSA algorithm can only handle 276 bytes of data.

Due to both ElGamal and RSA's limitations. The ECC algorithm, which has different curve specifications (secp128r1, secp128r1, secp192r1, and secp256r1), is the only option for encryption of small, medium and large datasets.

HARDWARE AND SOFTWARE REQUIREMENT

We have created and are running the CSU Application, CA Server, and CSP Server on an Intel Core i3 processor with 2 GB of RAM. Additionally, we tested the prototype of our system on the common/ordinary machines to demonstrate that it is more affordable and compatible with standard PCs.

METHODS AND MATERIALS

PROPOSED SYSTEM

Our developed system provides security for data in transit and data in storage from CSU to CA Server, CA Server to CSP Server, CSU to CSP Server, and vice versa. Our system uses SSL for communication security from point to point and end to end. Data that has reached plaintext must then be stored using encryption. Encryption is one of the primary security methods offered by our designed system. It is a very effective and useful approach to protect the data being carried over the network. Data is encrypted by the sender using a secret key, and only the designated recipient is able to decrypt the data using secret key. The legitimacy of the information is guaranteed by a digital signature. A digital signature is an e-signature that it establishes who sent the data. The use of a digital signature assures that the delivered data maintains its original content [9]. The original data is first passed through a hash value algorithm by the digital signature creation system, and then it is encrypted using a private key. Changing fixed-length characters into shorter-length values or keys that represent the original data that has been modified is a process known as hashing. Message Digest (MD2, MD3, MD4) and Secure Hash Algorithm (SHA-160, 256 and 512) are hashing and message digesting functions available.

For data at motion, the Secure Sockets Layer (SSL) protocol is used to encrypt data so that it cannot be read during communication between clients and servers over the Internet. SSL also provides privacy, integrity, and authentication. SSL employs the server certificate to furnish the client with the server's identity for verification; when the identity has been verified once, they exchange the public key. The SSL session uses the public key for encryption. In this form of communication, message digests are used to check that data hasn't been tempered, hacked, or altered in any way. Sessions for SSL operate through TCP. The SSL session is established via the TCP connection using TCP Socket. Data is encrypted during transmission through SSL and decoded at the receiving end. Secure point-to-point connections between computers are the main use for SSL [10].

Our developed system employs the RSA algorithm (Rivest-Shamir-Adleman). In 1977, the RSA algorithm was created. Public and private keys of RSA are generated using technique of multiplying two large prime numbers that can be divided by 1 or itself once keys generated then no longer use. RSA Private Key is used for decryption, whereas RSA Public Key is used for encryption. The RSA Private Key is used for Digital Certificates to sign data from CA and is used to sign encrypted data to demonstrate the validity of the data. The authenticity of digital signatures and digital certificates is checked using the RSA Public Key [11].

Unified Modeling Language (UML) diagrams are used to show some of the created system's key features. Use case analysis to illustrate the system's primary functions as demonstrated in Figure 4.

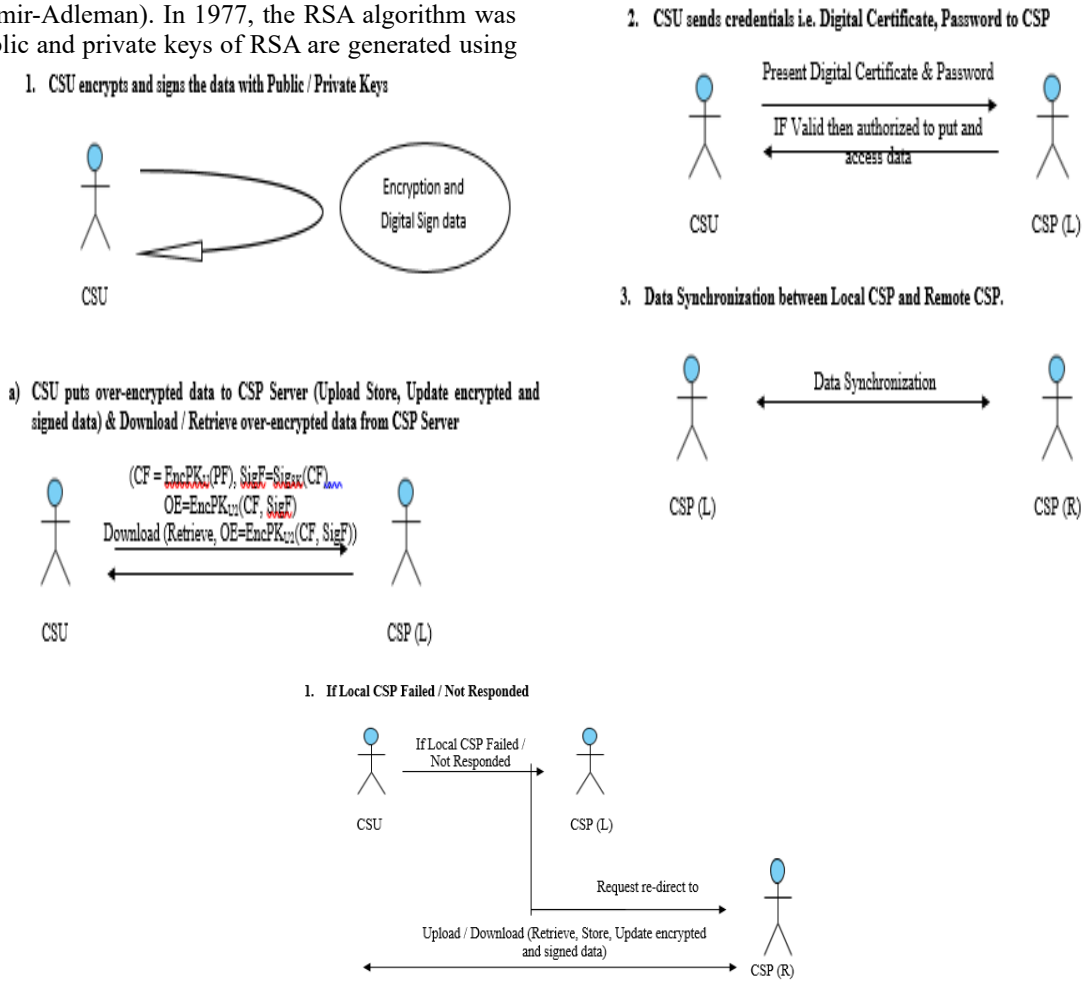

Figure 4: Use Case Analysis of System

Screen shots that show the execution of the process of decrypting the encrypted data and verifying its integrity using the public and private keys of CSU are shown as examples of the implementation. In the screenshot (Figure 5), CSU uses public and private keys to encrypt and sign the file and decrypt and verify the signature in order to ensure the data's integrity.

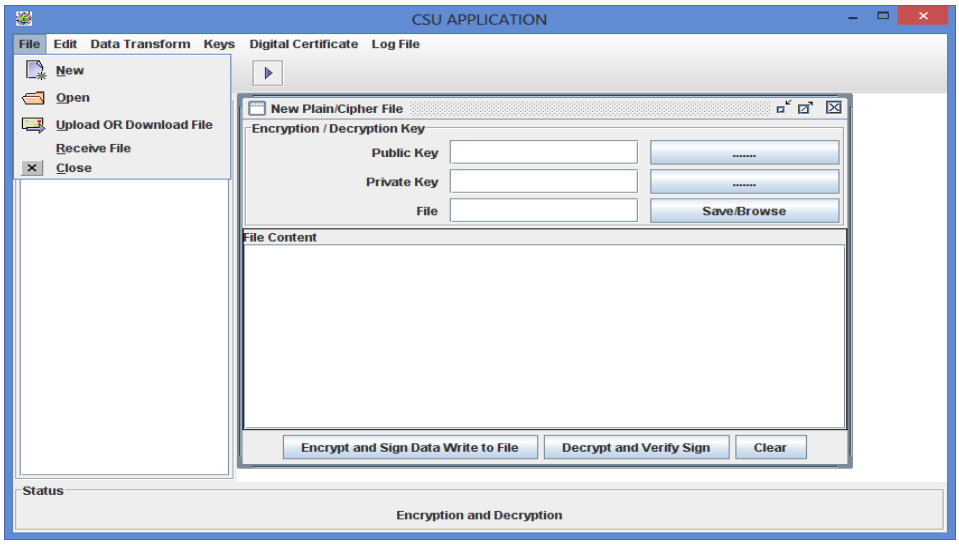

Figure 5: CSU Application

Figure 6 shows CSU uploads and downloads files after CSP verifies its authentication. If CSU's authentication is accepted, CSU is then permitted to upload and download encrypted and signed data to CSP Server.

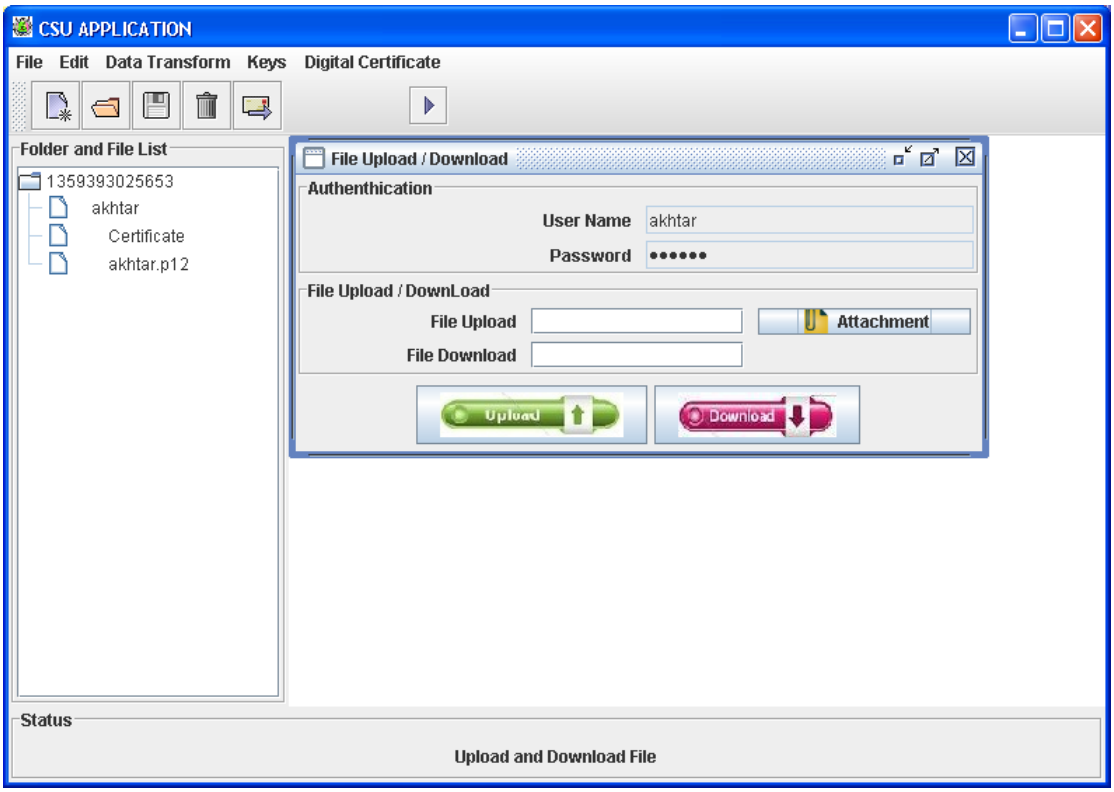

Figure 6: CSU Uploads / Downloads File to and from CSP

The main screen of CSP Server is seen in screenshot in Figure 7 which displays the options for logging information and many other helpful settings relevant to advanced systems.

Figure 7: CSP Main Screen

RESULTS AND DISCUSSIONS

A maximum key size asymmetric algorithms empirical comparison is presented that Comparative examination of maximum size asymmetric key pairs generation, the meanwhile for key pairs generation of ElGamal (256), DSA (1024), RSA (4096), ECC (secp521k1 & sect571k1) was in milliseconds, i.e., 754.2, 64.4, 4419.9, and 49 & 54 (ECC), as shown in Table 2. The result indicates that ECC takes less time to generate key pairs than other asymmetric techniques (i.e., ElGamal, DSA and RSA).

Table 2: Asymmetric algorithms key pair generation comparative analysis (Source: primary data)

	ASYMMETRIC CRYPTOGRAPHIC ALGORITHM				
	ElGamal (256)	**DSA (1024)**	**RSA (4096)**	**ECC (Prime)**	**ECC (Binary)**
Mean	754.2	64.4	4419.9	49	54
STDEV	407.593	1.075	1118.271	1.023	2.015

Figure 8 depicts a cooperative and comparative analysis of ElGamal, DSA, RSA, and ECC at the application level for symmetric secret key generation. DSA was discovered to be 485.704% quicker than ElGamal and 2846.415% faster than RSA. The findings revealed that ECC with curve specification prime fields (secp521k1) was 31.556% quicker than DSA, while ECC with curve specification binary fields (sect571k1) was 34.776% faster.

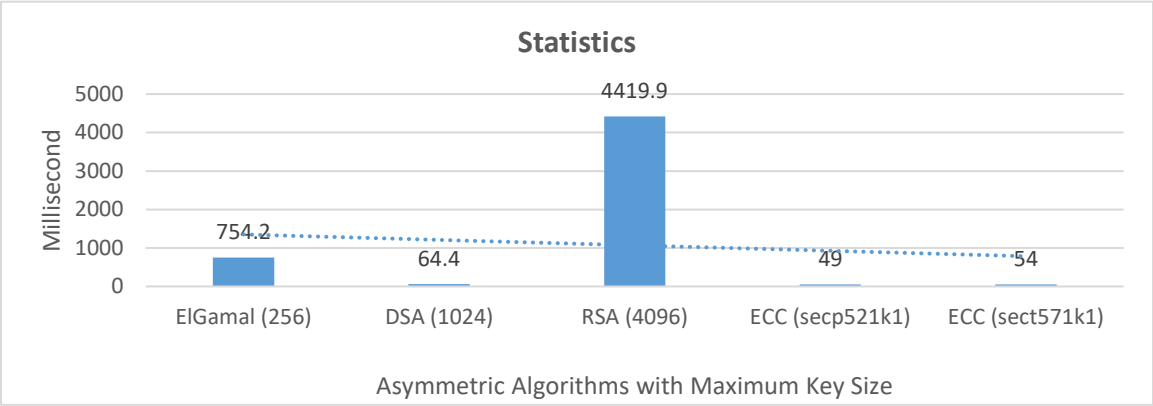

Figure 8: Asymmetric algorithms key pair generation comparative analysis

In asymmetric cryptography, encryption is the process of converting plaintext to ciphertext using the public key. The time was measured in milliseconds, i.e., 375.3, 5.5, and 2 correspondingly. The decryption using the private key of was 2.9, 58.6, and 198.2. It is clear from the results that ECC takes less time to encrypt than other asymmetric techniques. Meanwhile, it was discovered that ElGamal decryption took less time than previous asymmetric techniques, although data size was restricted to 16 bytes. With the same amount of data, RSA was quicker than ECC (Table 3).

Table 3: Asymmetric algorithms plaintext comparative analysis ((Source: primary data))

ASYMMETRIC CRYPTOGRAPHIC ALGORITHM						
	ElGamal (256)		**RSA (4096)**		**ECC (secp256r1)**	
	ENC	**DEC**	**ENC**	**DEC**	**ENC**	**DEC**
			Small Dataset			
Mean	1108	6	5.5	58.6	2	198.2
STDEV	78	2	0.527	9.913	0.471	32.424
			Medium Dataset			
Mean	-	-	13.3	160.2	4	1
STDEV	-	-	1.032	39.32	1	1
			Large Dataset			
Mean	-	-	-	-	5	2
STDEV	-	-	-	-	1	1

Figure 9 depicts the cooperative research of asymmetric algorithms with maximum key size in bits encryption and decryption, including ElGamal, RSA, and ECC at the application level for small plaintext datasets. ECC (secp256r1) was shown to be 175% quicker than RSA for encryption operations. Meanwhile, in the decryption procedure, ECC was 238.22% slower than RSA. ElGamal method with 256 bits key size was slower than ECC and RSA for encryption, but it was quicker than ECC and RSA for decryption. It can be inferred from the results that ECC (secp256r1) utilised less time for encryption operation as compared to others asymmetric algorithms with small dispersion from means it was reveals from recorded results that behaviour of data is consistent because data point tends to be very close, Decryption operation ElGamal during of time was smaller than ECC and RSA with small consistent behaviour.

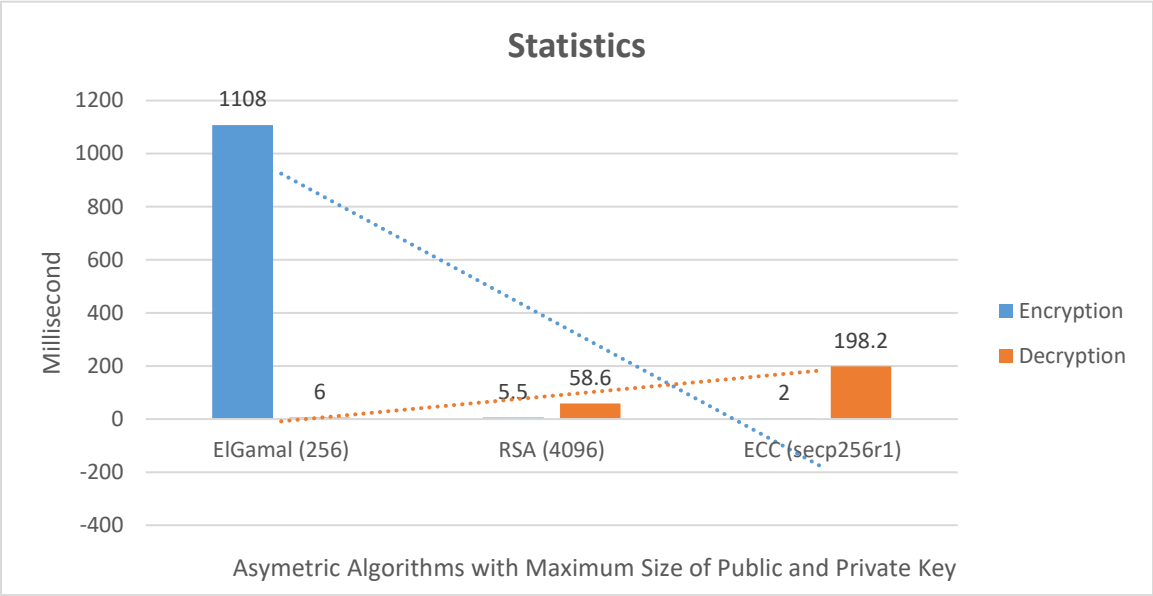

Figure 9: Asymmetric algorithms small plaintext comparative analysis

COMPARISON RESULTS IN PERCENTILE

Percentile defines how a value compares to other values in the same dataset. It is used for huge dataset values. The median is the same as the second quartile or fifteenth percentile. Percentile is a measure of performance in comparison to others; it is affected by the other numbers. It is based on the normal distribution of frequencies. A frequency distribution is the distribution of a collection of data in a table that shows the distribution of the data into classes or groups as well as the number of observations in each class or group. Table 4 summarises the results of the symmetric and asymmetric algorithms' key generation, encryption, and decryption in percentiles twenty-fifth, fifteenth, and seventieth (Quartiles Q1, Q2, and Q3):

Table 4: Percentile (25%, 50% & 75%) of Asymmetric algorithms

ASYMMETRIC CRYPTOGRAPHIC ALGORITHM												
	ElGamal (256)			**DSA (1024)**			**RSA (4096)**			**ECC (Prime)**		
	GEN	**ENC**	**DEC**	**GEN**	**ENC**	**DEC**	**GEN**	**ENC**	**DEC**	**GEN**	**ENC**	**DEC**
	Plaintext Small Dataset											
Q1	482.5	367	3	62.1	-	-	3624.5	5	52.5	49	2	182.75
Q2	590.5	375.5	3	64.4	-	-	4063	5.5	55	49	2	194
Q3	803.75	387	3	67.2	-	-	5161.5	6	64.5	49	2	227.75

It was discovered that ECC (secp256r1) was 175% quicker than RSA for encryption operations. Meanwhile, ECC was 238.22% slower than RSA in the decryption procedure. ElGamal method with 256 bit key size was slower than ECC and RSA for encryption, but it was quicker than ECC and RSA for decryption.

CONCLUSION

One of the main issues with cloud-based e-commerce and mobile commerce systems is security. The channel via which data are transmitted is insecure; any private information sent through these channels must be protected since, in cloud computing, data vulnerability is caused by storing data on remote servers, and data conceals from user in Public Cloud. The user loses control over the data and is unaware of where the data is stored. The security challenges that cloud computing confronts include data tampering, information leakage, eavesdropping and Man-in-the-Middle attacks. Our developed system provides personal data security, which includes data privacy, confidentiality, and integrity as well as secure cloud access. It also offers authentication and guards against eavesdropping. The system provides a safe and effective way to store and access data from Cloud applications, and our system ensures the

confidentiality and integrity of data sent to and stored by the Cloud. The developed system employs double-encryption that is over-encryption approach to address transmission issues and avoid eavesdropping attacks. Our system ensures the integrity of the data by checking for correctness. It can be inferred from the results that ECC (secp256r1) consumed less time for encryption operation than other asymmetric algorithms with small standard deviation recorded that indicate the behaviour of data is consistent because data point tends to be very close, Decryption operation ElGamal during of time was smaller than ECC and RSA with small consistent behaviour.

ACKNOWLEDGEMENT

We would like to express our sincere appreciation to everyone who helped and provided guidance while we completed this research work. This article was written by all contributors equally.

CREDIT AUTHOR STATEMENT

Dr. Mujeeb-ur-Rehman Jamali: Research Experiments, Implementation and Evaluation, **Dr. Shahmurad Chandio:** Writing Original Draft, Data Curation and Results Comparison and **Dr. Nadeem Ahmed Kansro:** Conceptualization and Methodology.

CONFLICT OF INTEREST

There are no conflicts of interest declared by the author.

REFERENCES

[1] T. Ramalingeswara Rao, Pabitra Mitra, Ravindara Bhatt, A. Goswami, "The Big Data system, components, tools, and technologies: a survey," in Springer Knowledge and Information Systems, vol. 54, no. 1, pp. 145-196, 2018. doi: 10.1007/s10115-018-1248-0.

[2] H. M. Deitel, P. J. Deitel and S. E. Santry, "Advanced Java 2 Platform, How to Program," Prentice Hall, Upper Saddle River, New Jersey, 2001.

[3] P. Ghazizadeh, R. Mukkamala and S. Olariu, "Data Integrity Evaluation in Cloud Database-as-a-Service," in IEEE Ninth World Congress on Services, pp. 606-613, 2013. doi: 10.1109/SERVICES.2013.100.

[4] P. Metri and G. Sarote, "Privacy Issues and Challenges in Cloud Computing," in International Journal of Advanced Engineering Sciences and Technologies, vol. 5, no. 1, pp. 001-006, 2011. ISSN: 2230-7818.

[5] K. Patel, "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files," in Springer International Journal of Information Technology, vol. 11, no. 4, pp. 437-445, 2019. doi: 10.1007/s41870-018-0271-4.

[6] M. Agoyi and D. Seral, "SMS Security: An Asymmetric Encryption Approach," in IEEE Sixth International Conference on Wireless and Mobile Communications, pp. 222-226, 2010. doi: 10.1109/ICWMC.2010.87.

[7] L. Dai and Q. Zhou, "A PKI-based Mechanism for Secure and Efficient Access to Outsourced Data," in Proceedings of International Conference on Networking and Digital Society, pp. 1-4, 2010. doi: 10.1109/ICNDS.2010.40.

[8] S. Sanka, C. Hota, and M. Rajarajan, "Secure Data Access in Cloud Computing," in Proceedings of IEEE International Conference on Communications (ICC), pp. 1-5, 2010. doi: 10.1109/ICC.2010.5502384.

[9] Z. Xu, C. Wang, Q. Wang, K. Ren, and L. Wang, "Proof-carrying Cloud Computation: the Case of Convex Optimization," in IEEE INFOCOM 2013 - IEEE Conference on Computer Communications, pp. 2831-2835, 2013. doi: 10.1109/INFOCOM.2013.6567032.

[10] J. Peng, X. Zhang, Z. Lei, B. Zhang, W. Zhang, and Q. Li, "Comparison of Several Cloud Computing Platforms," in Proceedings of IEEE Second International Symposium on Information Science and Engineering (ISISE), pp. 791-794, 2009. doi: 10.1109/ISISE.2009.213.

[11] H. M. Deitel, P. J. Deitel, and S. E. Santry, "Advanced Java 2 Platform, How to Program," Prentice Hall, Upper Saddle River, New Jersey, 2001.