JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Safety and Integrity of Computers within a Network Environment

Anjali[1]
Research Scholar (M.Tech)
Swami Sarvanand Institute of Engineering & Technology, Dinanagar
Punjab, India

Harjinder Kaur[2]
Assistant Professor
Swami Sarvanand Institute of Engineering & Technology, Dinanagar
Punjab, India

Abstract: ***The security and protection of computer systems and networks have become increasingly important in today's digital age. With the rise of cyber threats and data breaches, it is essential to have effective security measures in place to protect sensitive information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The security and protection of computer systems and networks involves various techniques, including encryption, firewalls, intrusion detection and prevention systems, and security policies and procedures. This topic encompasses a wide range of topics related to computer security and network protection, including threat intelligence, incident response, and penetration testing. The goal of computer security and network protection is to ensure the confidentiality, integrity, and availability of data and systems, while also complying with relevant laws and regulations.***

Keywords: Cyber security, Malware, Firewall, Encryption, Cyberthreat.

I. Introduction

In today's digital age, computer security has become a critical issue as more and more organizations and individuals rely on technology to store sensitive information, conduct business transactions, and communicate online. Security and protection of computer over network refer to the measures and practices put in place to ensure the confidentiality, integrity, and availability of information stored and transmitted over computer networks. Computer security threats can come from a variety of sources, including hackers, malware, viruses, phishing, and social engineering attacks. These threats can result in unauthorized access, data theft, system disruption, and financial loss. To protect against these threats, organizations and individuals need to implement security measures such as firewalls, antivirus software, intrusion detection systems, encryption, and access controls.

Network security also involves the protection of devices that are connected to a network, such as routers, switches, and servers. These devices are critical to the proper functioning of the network, and any compromise of their security can result in significant consequences. To protect network devices, organizations can implement security measures such as regular software updates, strong passwords, and access controls.

In summary, the security and protection of computer over network is a critical issue that requires constant attention and effort. It involves the implementation of various measures and practices to safeguard against threats and ensure the confidentiality, integrity, and availability of information stored and transmitted over computer networks.

Confidentiality

Confidentiality is a fundamental concept in information security that refers to the assurance that sensitive information is kept private and only accessed by authorized individuals or entities. It ensures that data remains confidential and protected from unauthorized disclosure, access, or interception.

In the context of information security, confidentiality focuses on preventing unauthorized users or adversaries from accessing, reading, or understanding sensitive information. This information can include personal data, financial records, trade secrets, classified documents, intellectual property, or any other information that should be kept confidential.

To achieve confidentiality, various security mechanisms and practices are employed, such as:

1. **Encryption:** The process of converting plaintext information into ciphertext using cryptographic algorithms. Encryption ensures that even if unauthorized individuals gain access to the data, they cannot understand it without the decryption key.
2. **Access Control:** Implementing measures to control who can access certain information or resources. This can involve authentication mechanisms like passwords, biometrics, or multi-factor authentication, as well as authorization controls to restrict access based on user roles or privileges.
3. **Data Classification and Handling:** Categorizing data based on its sensitivity level and applying appropriate controls to ensure that higher classified information is accessed only by authorized individuals or systems.
4. **Network Segmentation:** Separating networks and systems into different segments or zones based on security requirements. This prevents unauthorized access or lateral movement of attackers within the network.
5. **Secure Communication Channels:** Utilizing secure protocols like HTTPS, SSL/TLS, or virtual private networks (VPNs) to protect data during transmission over networks and prevent eavesdropping or interception.
6. **Physical Security:** Implementing physical controls like locks, access cards, surveillance systems, or secure data centers to protect physical assets and prevent unauthorized access.

Integrity

Integrity, in the context of information security, refers to the trustworthiness and reliability of data and systems. It ensures that data remains unchanged, uncorrupted, and authentic throughout its lifecycle. The principle of integrity focuses on maintaining the accuracy, consistency, and reliability of data and preventing unauthorized or unintended modifications, deletions, or alterations.

Integrity is essential to ensure that information is not tampered with, manipulated, or compromised, as this can lead to erroneous decisions, loss of trust, and potential security breaches. Data integrity can be compromised by various factors, such as human errors, malicious actions, hardware or software failures, or external attacks.

To ensure integrity, several measures and practices are employed:

1. **Data Validation:** Implementing mechanisms to verify the accuracy, completeness, and consistency of data. This can involve data validation checks, error detection and correction algorithms, checksums, or hash functions.
2. **Access Control:** Enforcing appropriate access controls to prevent unauthorized individuals or systems from modifying or deleting data. Access controls can include authentication, authorization, and accountability mechanisms.
3. **Backup and Recovery:** Performing regular backups of data to protect against accidental or intentional data loss or corruption. Reliable backup systems and disaster recovery plans are crucial to restore data to its correct state.
4. **Change Management:** Establishing processes and procedures for managing changes to systems and data. This ensures that modifications are properly authorized, tested, and documented, reducing the risk of unintended changes or unauthorized modifications.
5. **Secure Communication:** Utilizing secure communication channels, such as encrypted protocols, to protect data during transmission and prevent unauthorized modification or tampering.
6. **Cryptographic Hash Functions:** Applying cryptographic hash functions to verify the integrity of data. Hash functions generate a unique hash value for a given set of data, and any changes to the data will result in a different hash value.

Availability

Availability, in the context of information security, refers to the accessibility and usability of information, systems, and resources when needed. It ensures that authorized users can access and use data and services without interruption or significant downtime. The principle of availability focuses on maintaining the operational functionality and responsiveness of systems to support business operations.

High availability is crucial for critical systems and services, as any disruption or unavailability can lead to financial losses, reputational damage, or hindered productivity. Availability can be affected by various factors, including hardware or software failures, network issues, natural disasters, or malicious attacks.

To ensure availability, several measures and practices are employed:

1. **Redundancy and Fault Tolerance:** Implementing redundant components or backup systems to ensure continuous operations even in the event of hardware or software failures. Redundancy can include backup servers, data replication, load balancing, or failover mechanisms.
2. **Disaster Recovery Planning:** Developing comprehensive disaster recovery plans to handle major disruptions or outages. These plans include backup strategies, data restoration procedures, and alternative infrastructure options to minimize downtime and restore services quickly.
3. **Monitoring and Incident Response:** Deploying monitoring systems to continuously monitor the health and performance of systems and networks. This allows for proactive identification and resolution of issues before they impact availability. Incident response processes help address any disruptions promptly.
4. **Security Measures:** Implementing appropriate security controls to protect systems from attacks, malware, or unauthorized access that could impact availability. These measures include firewalls, intrusion detection systems, access controls, and security patches.
5. **Scalability and Capacity Planning:** Ensuring that systems have sufficient capacity to handle expected workloads and can scale up or down based on demand. This involves capacity planning, resource allocation, and performance optimization to prevent resource exhaustion and bottlenecks.
6. **Regular Maintenance and Updates:** Conducting routine maintenance activities, such as applying software updates, patches, and security fixes, to keep systems secure and prevent vulnerabilities that can impact availability.

II. Related Work

(L. D. Q. G. Ri & Dqg, 2020) The advancement of science and innovation, particularly the use of enormous information innovation, the job of PC networks has become increasingly critical. PC network significantly affects individuals' life and work, and has even turned into a piece of life and work. **(Jinquan, Al-absi, Al-absi, & Lee, 2020)**This paper initially sums up what data is, and afterward examination the assistance of data PC network security the board framework exhaustively. **(Tague, Member, Slater, & Member, n.d.)**As data innovation gradually infiltrates into individuals' day to day routines, the application scope of PC networks has become more extensive and more extensive, becoming one of the irreplaceable specialized techniques for individuals.**(Gao, Yang, Shi, & Zhang, 2019)**Current strategies for upholding security strategy rely upon security patches, against infection securities, and conflagration control, all refreshed in the end client's PC at truly diminishing spans.**(Bao, Wu, Yu, & Huang, 2020)**Data security is a broadly examined theme in the time of large information. With the quick improvement of PC networks, different data security issues have oftentimes happened. instructions to work fair and square of PC organization data security insurance through the execution of network security level insurance is the heading that organization It would be ideal for security to zero in on. **(Polytechnic, 2020)**With the rapid development of Internet technology, computer network technology has been applied in all walks of life, which is closely related to people's work and life. In the information environment, people's daily life and production methods have also changed accordingly. The application of information technology in people's daily life further enriches people's lifestyle and promotes the rapid development of social economy. **(Xiao, 2020)**The ceaseless improvement of organization innovation and data innovation, network has become a crucial piece of individuals' day to day routine and creation, and with the rising interest for network information. The fast advancement of PC network carries comfort to individuals lives, bitt it likewise delivers a progression of PC network security issues, which encroach on individuals' protection what's more, interests. Considering this, in view of the Web of Things, this paper examines the security of PC network data exhaustively, mostly investigates the security issues existing in the ongoing PC network Data, and advances some designated assurance methodologies, to guarantee the security execution of PC organization data and guarantee the dependable, nonstop and stable activity of PC network framework.

III. Proposed Work

- **RSA ALGORITHM:**

Step 1: Key Generation

1. Choose two distinct prime numbers, p and q.
2. Compute n = p * q. This value serves as the modulus for both the public and private keys.
3. Compute Euler's totient function: φ(n) = (p - 1) * (q - 1).
4. Choose an integer e (1 < e < φ(n)) such that e and φ(n) are coprime. e will be the public exponent.
5. Compute the modular multiplicative inverse d of e modulo φ(n). d will be the private exponent.

Step 2: Encryption

1. Convert the plaintext message into a numeric value, typically using a predetermined encoding scheme.
2. Compute the ciphertext c by raising the plaintext message m to the power of e modulo n: c = (m^e) % n.

Step 3: Decryption

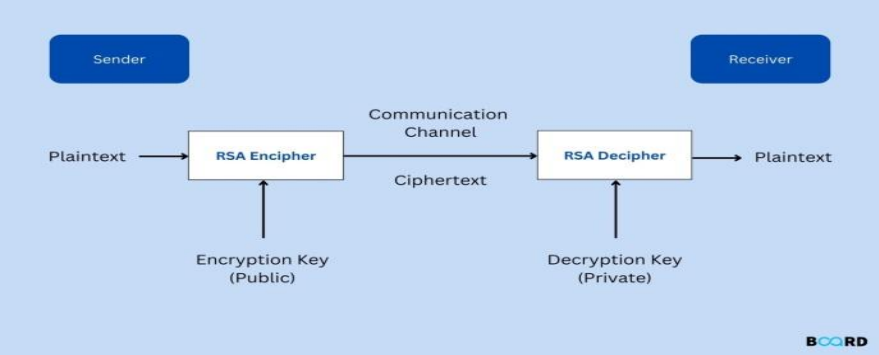
1. Receive the ciphertext c.
2. Compute the plaintext message m by raising the ciphertext c to the power of d modulo n: m = (c^d) % n.

Step 4: Security Considerations

1. Keep the prime numbers p and q secret. They should not be disclosed.
2. Store the private key (d, n) securely and share the public key (e, n) with the intended recipients.
3. Use sufficiently large prime numbers and key sizes to ensure the security of the RSA algorithm. Common key lengths for RSA encryption are 2048 bits or higher.

- **EXPLANATION OF RSA ALGORITHM:**

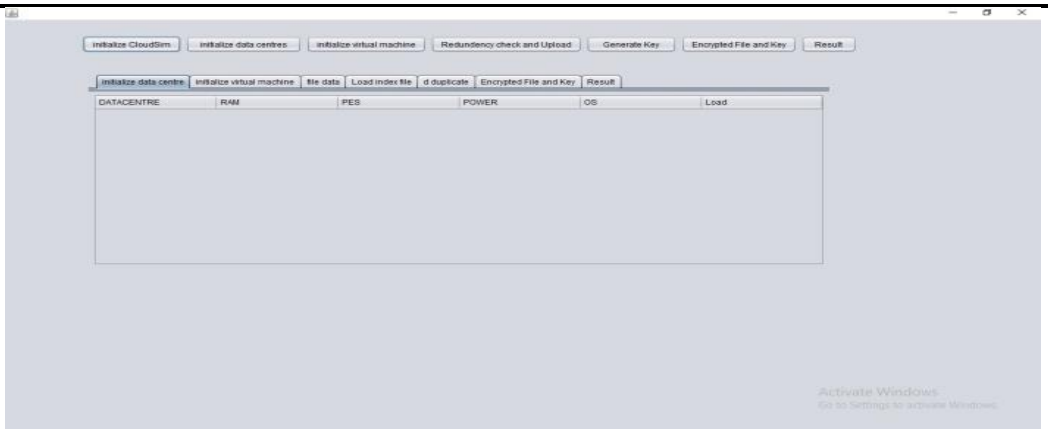
The security of RSA relies on the computational difficulty of factoring large numbers into their prime factors. The strength of the algorithm lies in the difficulty of determining the private key from the public key. It's worth noting that a proper RSA implementation involves additional considerations, such as padding schemes to address security vulnerabilities, handling of large numbers, secure random number generation, and protection against side-channel attacks.



RSA ALGORITHM DIAGRAM

IV. Result and Discussion

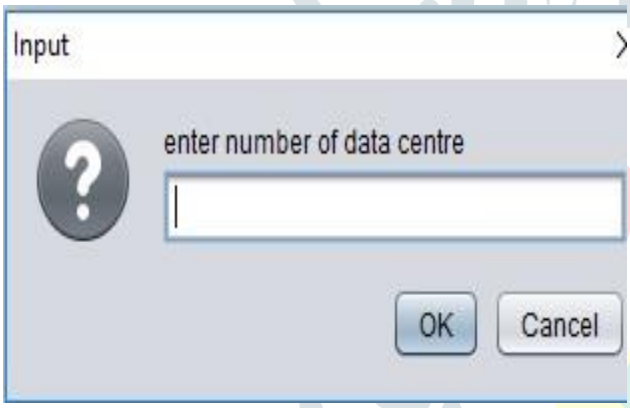
Initialize CloudSim: CloudSim is an open-source framework, which is used to simulate cloud computing infrastructure and services. It is developed by the CLOUDS Lab organization and is written entirely in Java. It is used for modelling and simulating a cloud computing environment as a means for evaluating a hypothesis prior to software development in order to reproduce tests and results. We Need to Initialize CloudSim first to make Datacenters and Virtual Machines and other related work.



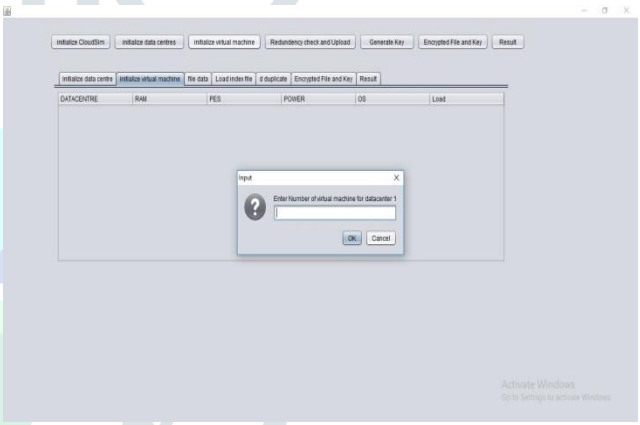
Initialize CloudSim

Initialize Datacenters: A data center - also known as a *data center* or *data center* - is a facility made up of networked computers, storage systems, and computing infrastructure that businesses and other organizations use to organize, process, store large amounts of data. A business typically relies heavily on applications, services, and data within a data center, making it a focal point and critical asset for everyday operations.

After Initialize CloudSim, we need to define number of Dataceters.

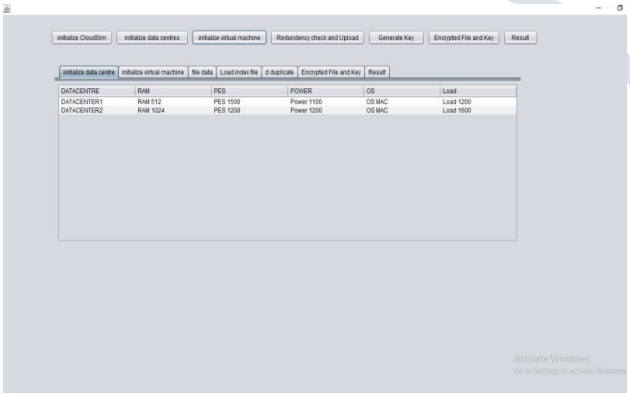


5.2 Input no. of DataCentres



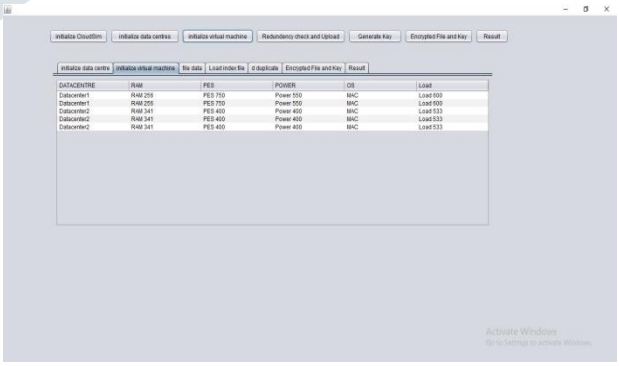
Input no. of Virtual Machines

The Following is a Detail of resources of Datacenters.



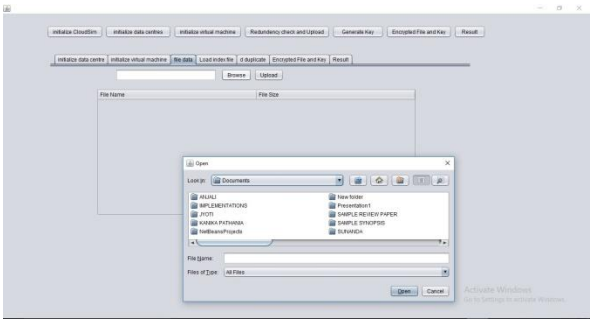
Displaying resources of Datacentres

The Following is a Detail of split resources of Datacenters as an Virtual Machines.



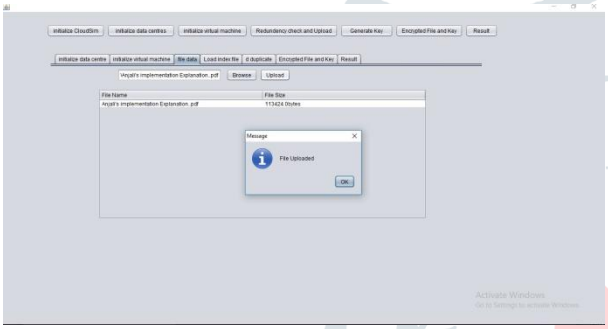
Detail of split resources of Datacenters as a Virtual Machines

In this Snapshot we upload file to upload for applying Encryption Key.



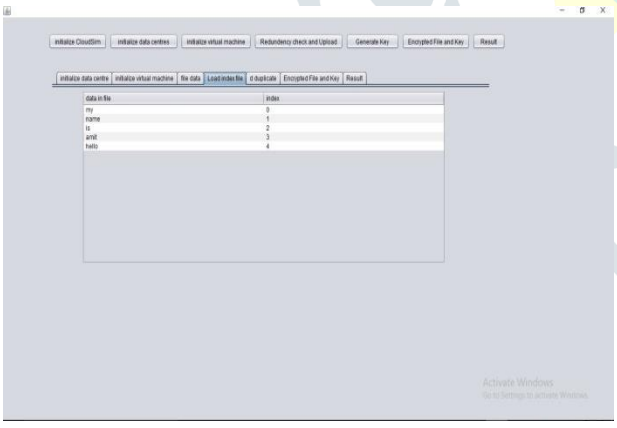
File Uploading for Processing

In Following Snapshot, File Upload Status with File Name and File Size is displayed.



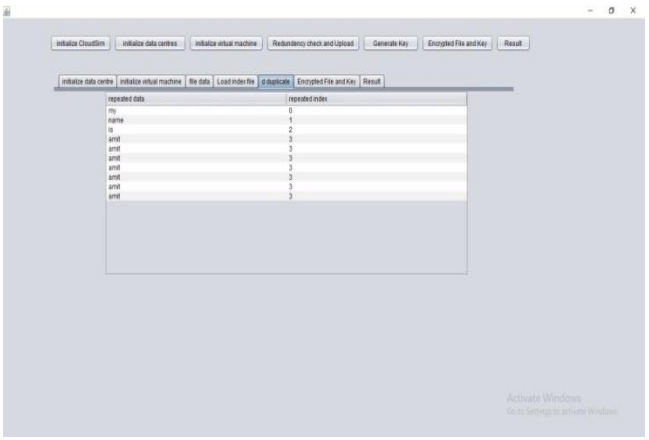
File Upload Alert Message

In the Following Snapshot, The uploaded file is indexed started from 0.



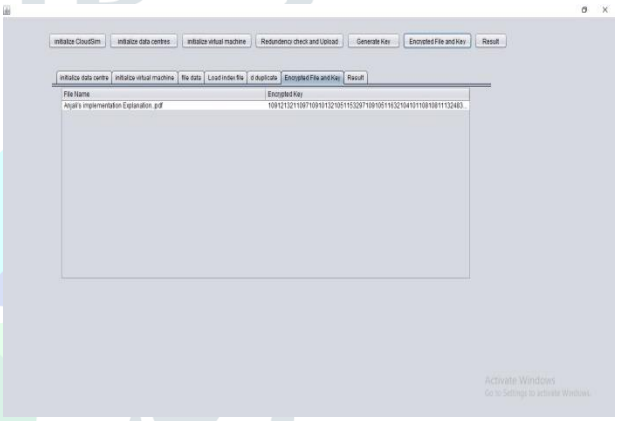
Load Index File

In the following, Duplicate words are displayed.



Duplicate words are displayed

In the Following, Encrypted Key is Displayed along with File Name.



Encrypted Key is displayed along with File Name.

In the Following, Result is displayed in Graphical form. The Existing Size of Encrypted Key is more and less secure and Preposed Size of Encrypted Key is less and more secure.

Proposed and Existing Result

V. CONCLUSION

The security and protection of computers over networks is crucial in today's digital age. With the increasing number of cyber threats, it is important to take measures to protect sensitive information and data from unauthorized access, theft, and misuse. To ensure the security of computers over networks, various security measures can be implemented, including the use of strong passwords, encryption, firewalls, antivirus software, and intrusion detection systems. Additionally, it is important to keep software and operating systems up to date to prevent vulnerabilities from being exploited by attackers. Furthermore, user awareness and education play a vital role in enhancing the security of computers over networks. Users should be educated on safe browsing practices, avoiding suspicious links, and identifying phishing emails.

VI. REFERENCES

1. Adi, K. (2008). Formal Modeling for Security Behavior Analysis of Computer Systems ∗, 49–59. https://doi.org/10.1109/MCETECH.2008.20
2. Bao, L., Wu, S., Yu, S., & Huang, J. (2020). Client-side Security Assessment and Security Protection Scheme for Smart TV Network, 573–578.
3. Chunli, L., & Donghui, L. (2012). Computer Network Security Issues and Countermeasure V, 328–331.
4. Dong, L., Peng, X., Zhuang, Y., Zhu, Z., Xu, H., Zheng, L., … Zhang, Y. (2020). Research on Computer Security Protection Technology Based on Information, 459–464.
5. Dqj, L. Q. J., Kdqj, H., Dqj, D., Dq, L., & Ldqj, X. (n.d.). 6HFXULW \ DQG 3URWHFWLRQ 6WUDWHJ \ % DVHG RQ , QWHUQHW RI 7KLQJV, 5–8.
6. Gao, P., Yang, R., Shi, C., & Zhang, X. (2019). Research on Security Protection Technology System of Power internet of things, (Itaic), 1772–1776.
7. Guo, Y., Xu, J., Yuan, H., Zhuang, Y., Zhu, G., & Zhang, Y. (2020). Research on Enterprise Computer Network Security Protection Technology Based on Information Technology, 488–491.
8. Hu, C., & Lv, C. (2010). Method of Risk Assessment Based on Classified Security Protection and Fuzzy Neural Network, 462–465. https://doi.org/10.1109/APWCS.2010.103
9. Jiang, W., Fang, B., Zhang, H., & Tian, Z. (2009). Optimal Network Security Strengthening Using Attack-Defense Game Model, 475–480. https://doi.org/10.1109/ITNG.2009.300
10. Jinquan, J., Al-absi, M. A., Al-absi, A. A., & Lee, H. J. (2020). Analysis and Protection of Computer Network Security Issues. *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, 577–580.