MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6635-6638

A SYNERGISTIC APPROACH TO SOCIAL CHATTING WITH EMBEDDED COMPRESSION AND ENCRYPTION MECHANISMS

Shefali Arora and Sherry Verma
School of engineering and technology
Sushant University (Erstwhile Ansal University) Gurugram, India
shefaliaroraphd@gmail.com
sherryverma@sushantuniversity.edu.in

ABSTRACT

Digital Era is often referred to be the age of the most recent information technology, and it is at this time that internet services have become more popular for the purpose of providing a social chatting system. It has been noticed that the present digital age is impacted by the frequent use of social platform, which is imparting knowledge to users. This finding supports the hypothesis. In the context of the current situation, it is clear that social platform is playing a big role in the dissemination of talking. Simply issuing few simple commands is all that is needed to quickly get the necessary information. People make frequent use of many social platforms on a daily basis, including Facebook, Whatsapp, Twitter, and Telegram, among others. These platforms are functioning rather well as useful tools for social chatting systems. The use of such platforms has hastened the process of conversing due to their acceleration. In this work, we investigate the influence that compression and encryption will have on social chatting systems in the age of digital technology. Existing pertinent research on social chatting and the obstacles posed by using such a system have both been taken into consideration in this study. The main problems associated with utilizing social media as a medium for conversing are the lack of dependability and authenticity. In addition, since the platform is available to anybody, it is now simpler for individuals to offer their points of view on a certain subject. However, this is made more difficult to comprehend as a result of competing hypotheses that are provided by experts in a variety of professions.

Keywords—Social Chatting System, Compression, Encryption, social platform

1. INTRODUCTION

Since the introduction of the internet, the majority of our communication is now carried out through the displays of our personal computer monitors or even via the phones in our pockets. One of the many improvements to this was an application for chatting, which enabled immediate conversation with anybody located in same city, in different state, or anywhere else on world. This was only one of the many enhancements. Especially in light of the meteoric rise in popularity of chatting applications, the standard SMS text message is rapidly becoming an obsolete form of communication. Free text messaging is available via a variety of programmes such as WhatsApp, Telegram, and Viber. In addition to that, this does not even take into account fact that there are other alternatives for voice & image sharing across various customers. The use of messaging and chatting apps has evolved into a way of life. They give off the impression of being a more reliable mode of communication than a phone call would be.

1.1 Social Chatting System; A "chat" is any kind of online conversation, discussion, or message passing. The participants are two or more people chatting online or via a chat-enabled service or application. The word "chat" refers to a spoken exchange between two people through a network connection. Online chitchat may take the form of textual, spoken, aural, visual, or audio-visual (A/V) exchanges. If you want to have a chat session from your desktop computer, you'll need an instant messenger or Internet Relay Chat (IRC) client, both of which need a centralised server to facilitate chat conversations between individual users' devices. There are additional chat rooms available online, albeit these often need a user to have an email account to join. The moment a user registers, they have the option of either entering a public chatroom or sending a personal message to another member of the community. The conversation operations in an online chat service are managed via chat interfaces designed specifically for that purpose.

1.2 Data Compression: A procedure that decreases the amount of data by eliminating unnecessary or redundant information from it is known as data compression. It does this by lowering the amount of redundant data representation, which in turn lowers the amount of storage space needed for that data. Additionally, it lowers the cost of transmission by making more efficient use of the bandwidth that is available. There are a variety of ways for compressing data that may be used for a variety of file types, including text, audio, video, and picture files. Lossy compression and lossless compression are the two most common types of data compression. However, integrity of the data is going to be maintained even while using lossless data compression. Data compression is a procedure that may be used to compress any kind of material, including text, audio, and video, to the point that the original file can be entirely recovered without any real information being lost in the process. If one wishes to reduce the amount of space used up by storage, one might find that this technique is helpful. It is quite simple to trade compressed files over the internet due to the fact that these files may be sent or downloaded considerably more quickly. The areas of file storage and distributed systems are two of the most significant areas where data compression may be used.

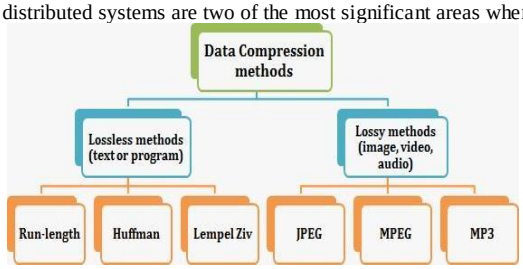

Fig. 1. Data Compression

In the realm of multimedia, as well as in text documents and database tables, data compression is used. Lossy methods and lossless techniques are the two primary categories that may be used to classify the many types of data compression techniques. Lossy data compression refers to the process of compressing data using an algorithm that discards some of the original data. The process of compressing data without losing information is termed lossless data compression, and the technique that accomplishes this goal is called a lossless data compression algorithm. The practise of compressing data to a smaller number of bits than its initial representation in order to reduce the amount of storage space it requires and the amount of time it takes to transmit it over a network is referred to as data compression. Data compression is feasible because to the fact that the vast majority of data in the actual world is highly redundant. In order to transform data from a format that is simple to work with into one that is more space-efficient, a compression application is used. A software that uncompresses data does the same thing, restoring it to the shape it was in before it was compressed. Numerous proposals and implementations of lossless data compression algorithms have been made. The Shannon-Fano algorithm, the Huffman coding method, the run-length encoding method, and the arithmetic encoding method are some of the most important approaches. Computing on the cloud is becoming an increasingly popular topic of investigation among academics in the modern world. Cloud computing is often regarded as a potentially fruitful alternative for mobile computing because to the many advantages that it offers in terms of quality, mobility, and connectivity. Mobile cloud computing has gained importance as a result of the growing need for mobility in cloud computing.

1.3 Encryption: Social chats are lengthy conversations between users of many apps that are encrypted. However, users have not been provided with a means to save a backup of the chats that are stored in the cloud.

ECDH key exchange is meant to provide the key pair that will be transferred between the two parties and produce the safe shared key that will be used as a key for the encryption algorithms, enabling end-to-end encryption. To accomplish this, End-to-End Encryption is a property that must be achieved. Confidentiality, Encryption is the method that ensures that communications between two parties remain private. Achieving this aim requires using encryption. The symmetric algorithm encrypts a communication, and the recipient of the message is the only one who is able to read the encrypted version of the message. The suggested application is successful in achieving privacy, which is one of the most important operators. Metadata, which includes a user's location, name, and contact information, is not collected. In addition to data about the service itself, metadata might also include data about the user's device. The suggested application safeguards data by ensuring that no changes were made to a message while it was sent. If an enemy were to alter the message in any way, or even replace it altogether, the original message would likely not be seen. Through the use of ECDH key exchange, we achieve end-to-end encryption while keeping performance at a high level by encrypting data using symmetric encryption methods (AES and RC4). This aids in preserving the functionality and performance of the mobile CPU.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6635-6638

1.4 Role of in Encryption in Social chatting system using Compression

When you save data on certain tape devices, the data is compressed using the device's specific compression algorithm. Data that has been encrypted should not be able to be compressed, since this contradicts the very notion of encrypted data; if you are able to compress encrypted data, then it is definitely not very properly encrypted. You may reduce the size of your data before encrypting it by making use of the Compression option that is available inside Encryption Services. Patterns are essential to compression's ability to achieve any size reduction at all.

Fig. 2. Role of in Encryption in Social chatting system using Compression

If you apply the compression technique on data that has been encrypted, you won't see much of a size decrease, if any at all; this is because encryption eliminates patterns like the one shown above. At a high level, data compression seeks to make advantage of recurring patterns within the data in order to decrease the amount of data. When data is encrypted, it is reorganised in such a manner that, in the absence of the decryption key, it is impossible to discern any patterns in the data. Encryption results in output that has the appearance of being random; specifically, a tangle of bits with a high level of entropy. Encryption, in its most basic form, refers to the act of encoding data in such a way that it is concealed from or unavailable to those who are not permitted to see it. When data is compressed, it takes up less space in storage, speeds up file transfers, and reduces the amount of money spent on storage hardware and network bandwidth. To turn (information or data) into a cypher or code is what it means to encrypt, and this process is often done to prevent unwanted access. Lossless and lossy are the two categories that describe the many compression methods. Both lossless and lossy compression are used often, with ZIP archive files serving as an example of the former and JPEG picture files serving as an example of the latter.

2. LITERATURE REVIEW

M.E. Alex and his fellow employees (2017) An infrastructure for cloud computing forensics. In recent years, there has been a rise in the popularity of cloud computing due to the fact that cloud resources are not only shared by numerous users but may also be deployed on demand. According to recent research, cybercriminals have been successful in abusing cloud computing technology due to the intrinsic features of the technology as well as a lack of cloud-specific digital forensic tools. This was revealed by the study. When it comes to preventing crimes committed in the cloud, cloud forensics provides investigators with a variety of challenges and concerns. Challenges that forensic investigators face are described in detail. Cloud Service Providers (CSPs), who are the subject of the vast majority of research studies, are the primary factor that determine the success of forensic investigations conducted in the cloud. The collection of forensics data is dependent on CSP, and any changes made to that data might potentially have a domino effect throughout the investigation. One method that may be used to reduce dependency on CSP is the development of a fresh plan to collect forensic evidence in locations other from cloud environments.

N. Smart et al. [2] (2010) Encryption based on homomorphism that has a small key and cypher text size. The following demonstrates fully homomorphic encryption with very small key and cypher text sizes. Following Gentry's methodology, we begin with a "somewhat" homomorphism scheme and then proceed to turn it into a totally homomorphism scheme. The cypher text is each constructed out of a single large integer in the relatively homomorphism system. This particular integer serves as the common denominator for the public key and the private key. This indicates that the size of the keys and message expansion in our method is less than those in Gentry's original technique. Our proposal's cheap full homomorphism encryption makes it feasible to encrypt data over any field with characteristic two Gonzales D et al [3] (2017) Clouds that provide infrastructure as a service (IaaS) may be evaluated with the help of the Cloud-trust model. Concerns have been raised by both the government and private industry over susceptibility of CCS to APT. The Cloud-Trust evaluation approach uses our cloud architecture reference model, which incorporates a number of different security safeguards and best practises, to estimate high-level security metrics in order to conduct an evaluation of a CCS provider's level of confidentiality and integrity.

It is anticipated that Eduardo Giometti Bertogna et al. will present their findings in the year 2020. This study presents advancements in Mobile Cloud Computing (MCC). The goal of this study is to find a solution to these challenges by utilising these technologies. The use of the CPU on the mobile device was decreased by the use of vector quantization for the purpose of ECG signal reduction. The performance of the system was evaluated and found to be suitable for the remote ECG monitoring of patients, with very minimum signal distortion. This was accomplished by lowering the bandwidth requirements. Architecture of this system as well as the concepts presented here might be implemented in telemedicine systems.Within the body of work done by Z. Xiao and others (2013) Protecting one's privacy when using cloud computing. As a consequence of recent developments in technology, cloud computing has seen a rise in both its popularity and its level of economic success. On the other hand, handing over control of one's data and one's company's apps to a third party raises additional levels of privacy and safety issues. The major objective of this study is to provide a thorough analysis of the issues surrounding cloud computing security and privacy. Security and privacy are the two most prominent features of secrecy. Examining these features, their interdependencies, the potential weaknesses that may be exploited by attackers, the threat models, and the defences in place are all crucial in the context of a cloud environment. Each characteristic comes with its own individual possibilities for further research in the road.The group led by Dr. Dhirender Singh, included his colleagues There is something known as cloud computing. In order for cloud computing to be widely adopted by a wide variety of users, this research has looked at a number of different methods that ensure data security. These mechanisms need to be generally acceptable. In addition to this, it offers a summary of current research subjects in cloud computing as well as possible advances in the near future. It is possible that cloud computing will become a popular research subject in the current climate. Cloud computing is an appealing option to mobile computing for a variety of reasons, including its mobility, quality, and connection. The need for mobility in cloud computing may be credited with contributing to the value of mobile cloud computing.

R. Latif and his fellow employees [7] The article "Cloud computing risk assessment: a complete literature study" was published in Future Information. The study of cloud computing security covers an extraordinarily wide range of topics, from the protection of cloud data and resource access to the defence of cloud hardware and platform technologies. Even though advantages of cloud computing are considerable, many cloud customers have voiced concerns about the level of security and privacy it provides, which has slowed the widespread adoption of cloud computing by enterprises and other organisations.

B. S. Rawal et al (Mar. 2018) [8] "developer of a proxy re-encryption system for the storage and exchange of files in the cloud. Cloud computing services not only provide an enormous amount of storage space, but they also do away with the need that users have data stored on their own personal computers. Companies that offer cloud storage say they are able to provide data storage that is both flexible and safe, and that can be adapted to satisfy a broad variety of storage needs. The majority of security technologies have a limited rate of failure, and incursions are occurring in more intricate and sophisticated methods; thus, the security failure rates are quickly growing. After our data has been transferred to the cloud, we will no longer have control over it; as a result, the cloud poses new risks to the data's confidentiality and authenticity.Researchers Sadok L and colleagues (2017) [9] are saying that. Management of software programmes using a compositional approach. Noisy computing is something that may especially pique the curiosity of researchers working in today's environment. Cloud computing is an appealing option to mobile computing for a variety of reasons, including its mobility, quality, and connection. The need for mobility in cloud computing may be credited with contributing to the value of mobile cloud computing. This study looked at a variety of different methods for assuring the safety of data in the cloud to facilitate widespread adoption of cloud computing among a wide variety of users. In addition to this, it offers a summary of current research subjects in cloud computing as well as possible advances in the near future.In S. Amamou et al. [10] 2019, "2019: a watershed year for data protection in cloud computing A successful public cloud architecture includes data protection that guarantees the system is operating as expected for cloud users as well as cloud providers alike. Even yet, not nearly enough thought has been put into the process of protecting individuals' private information. When data is retrieved from the cloud after being transmitted between cloud services, the data may be exposed to a possible risk. As a consequence of this, we detailed a number of well-documented attacks and then analysed the many strategies that have been offered in the literature for minimising the effect of these assaults.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6635-6638

According to the findings of Tosaporn Srisooksai and colleagues [11] As one example of a potential solution, efficient media access control or routing protocols have been proposed. One of the strategies that is suggested for use in order to cut down on the quantity of data that is sent via wireless networks is the data compression system. Inter-node communication, which is typically what takes up the majority of the energy in wireless sensor networks, is required less and less. This article takes an in-depth look at the different data compression algorithms that are presently being utilised in wireless sensor networks and gives an analysis of each one. Appropriate criteria sets need to be constructed before current tactics can be identified, and before decisions can be made about what the best method of data compression for wireless sensor networks should be. This is a really crucial point. After that, we will proceed to discuss the particulars of each kind of compression in more detail. Their performance, open problems, restrictions, and possible applications in wireless sensor networks are analysed and compared as the last phase in the process.

To name only a few examples: Bogdan Batrinca et al. [12] This article is for you if you work in the area of social science and are interested in learning more about the many forms of social media that are available in today's world. A comprehensive look is taken at several software applications. Because we want to provide as much information as possible, we have included introductions to social media. This evaluation also includes a comprehensive look at the technology pertaining to social media platforms. Because of the availability of web-based APIs from Twitter, Facebook, and news services, research and industry are increasingly concentrating their attention on analysing Twitter feeds for sentiment analysis. This is due to the fact that Twitter is one of the most popular social media platforms. 2016 study by Hui Cui and colleagues [13], It demonstrates attribute-based encryption that has both revocability and decentralisation. The authors ABE system that is both revocable and decentralised. This technique removes the requirement for a centralised authority by allowing attributes to be revoked via the cessation of private key updates. Our solution makes it simple for any trusted third party to issue and periodically update private key components for users, giving them the appearance of being an AA. When an AA's attribute is removed, it might depart the system without informing any other AAs or triggering any global communication. Stopping the process of key updating for a specific account may also be used to revoke access to that account without having an effect on the functionality of any other accounts. In order to construct our system, we need to find a solution to the technical difficulty of assuring that the confidentiality of private keys cannot be breached.In 2016, Hui Cui and colleagues [14] reported on their findings. Attribute-based encryption with server support. Attribute-based encryption (or ABE for short) is a one-to-many public key encryption solution that makes granular access control to encrypted data stored in the cloud a practical possibility. However, removing a user's access in ABE has proved to be a difficult and time-consuming endeavour. Boldyrev, Goyal, and Kumar devised a revocation technique that relies on a binary tree data structure and fuzzy identity-based encryption to address this problem. A key generation centre (KGC) is a centralised location that updates all of the data consumers on a regular basis with new key information over a publicly accessible channel. Since it reduces the frequency of key updates from a linear function of the number of users to a logarithmic function, it has seen widespread implementation in upcoming revocable ABE systems. However, it's crucial that all non-revoked users regularly update their decryption keys for each new time period and that each user has a private key whose size is proportionate to the logarithm of the data.(2013) [15] "Dong and associates." [Citation needed] employing fuzzy keywords to search through encrypted data in public key setup. When data that has been encrypted is stored on cloud servers, is used to facilitate the searching of the encrypted data. You are only able to search for very precise terms when using classic searchable encryption; you cannot search for more general keywords. A new evolving paradigm known as fuzzy keyword searchable encryption is being proposed as solution to this problem. When it comes to public key cryptography, on the other hand, the only algorithms that have been presented for fuzzy keyword search are inefficient ones. IPEFKS, or interactive public key encryption with fuzzy keyword search, is an unique primitive that offers effective fuzzy keyword search in an environment that uses public keys. An IPEFKS-based homomorphic encryption system is designed and developed by our company. Implementing LWW-FKS, is the most effective scheme that is now being used, in order to compare it to the other schemes that are already in use will allow for this comparison. When compared to LWW-FKS in terms of performance, IPEFKS is much more efficient.

A number of people, including Kolo, Jonathan Gana, and others, have contributed to the writing of this research (2012) [16]. A technique of data compression for wireless sensor networks that is both flexible and does not suffer any data quality degradation. Due to the fact that sensor nodes are often powered by batteries, which have a finite amount of storage space, wireless sensor networks (WSNs) need careful consideration of energy usage.

3. NEED OF ENHANCEMENT OF PERFORMANCE OF SOCIAL CHAT SYSTEM

The Internet-based delivery of a wide range of services is at the core of Social Group's goal. IT infrastructures are made up of various components, including storage, servers, databases, networks, and software. As long as a computer has Internet connectivity, data and applications may be downloaded. This means that secure cloud storage must be implemented on top of a public cloud architecture where users do not have entire confidence in the service provider. Reduce the amount of data by removing extraneous information and compressing it. Text, audio, video, and image files may all be compressed using a number of ways. The increased value of mobile cloud computing may be attributed to the increased demand for cloud computing mobility. This comprehensive examination examines a wide range of social networking and wiki software, as well as basic syndication feeds, blogs, and newsgroups. This evaluation also includes an in-depth examination of social media technology. The suggested investigations are predicated on the premise that they would solve the problems that plagued previous research. Accuracy and velocity might be enhanced with more study. In order to safeguard the identification machine language for intestinal automation, this study proposes to employ Increase in Popularity of Safe, Low-Bandwidth Cloud-Based Social Chat.

4. PROBLEM STATEMENT

For industrial automation, there have been various studies in the area of Secure & Light Weighted Cloud Based Social Chat Grow to protect identification, however they have some limitations. A lack of focus on accuracy and performance was seen in previous studies. Furthermore, these studies were unable to deal with real-world problem. Those studies have a restricted scope and are unable to adapt to changing circumstances. However, there have been a number of researches Secure & Light Weighted Cloud Based Social Chat Grow although with certain limitations. Pervious investigation revealed a disregard for precision and effectiveness. In addition, these researches were unable to address an issue that exists in the actual world. Studies like this are constrained by their scope and so unable to respond to shifting conditions.

5. RESEARCH METHODOLOGY

This research was unable a capable to resolve the issues of pervious research. This research has provided better accuracy and performance. This research is applicable in real-life scenario. Those research have limited scope and lack of flexibility solution with width scope . According to the planned studies, they would be able to solve the issue of past research. The Internet-based delivery of a wide range of services is at the core of Social Group's goal. IT infrastructures are made up of various components, including storage, servers, databases, networks, and software. As long as a computer has Internet connectivity, data and applications may be downloaded. This means that secure cloud storage must be implemented on top of a public cloud architecture where users do not have entire confidence in the service provider. Research like this might lead to improvements in both accuracy and speed. Secure & Lightweight Cloud Based Social Chat Grow is used to safeguard the identifying machine language for intestinal automation in the suggested job. Options and flexibility abound in the planned project.

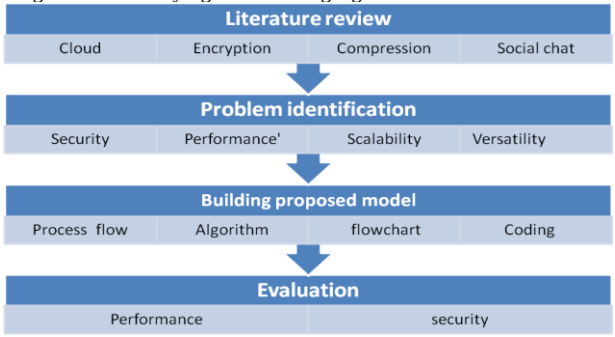

Fig. 3. Proposed Research Methodology

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6635-6638

Mathematical Equations Used in the Proposed System

1. Compression Ratio (CR)

Measures the effectiveness of compression:

$CR = S_{original} / S_{compressed}$

Where:

- $S_{original}$= Size of original data
- $S_{compressed}$= Size after compression

Higher CR ⇒ Better compression efficiency

2. Data Reduction Percentage (DR)

$DR(\%) = (S_{original} - S_{compressed}) / S_{original} \times 100$

3. Encryption Function (AES / RC4)

$C = E(K, D)$

Where:

- (C) = Cipher text
- (E) = Encryption algorithm
- (K) = Secret key
- (D) = Plain data

4. Decryption Function

$D = D(K, C)$

Where:

- (D) = Decrypted data
- (C) = Cipher text

5. ECDH Shared Key Generation

$K_{shared} = d_A \times Q_B = d_B \times Q_A$

Where:

- (d_A, d_B) = Private keys of sender and receiver
- (Q_A, Q_B) = Public keys

6. Transmission Time (Latency)

$T = S_{compressed} / B$

Where:

(T) = Transmission time

(B) = Available bandwidth

7. Security Strength Indicator

Security x (Key Length / Attack Feasibility)

Indicates increased security with stronger keys and encryption.

8. Overall System Efficiency

$\eta=\alpha(CR)+\beta(Security)-\gamma(Latency)$

Where (α, β , γ) are weighting factors.

6. NEED OF RESEARCH

A social network is not only a venue where individuals may interact with one another and develop connections; rather, it is much more than that. Because to cloud computing, companies that specialize in social networking no longer have to construct and maintain their own individual computer infrastructures. The terms "cloud" and "social" are working together to give members of social networks with a sustainable environment in which they may share resources. This research provides an introduction to cloud computing that is based on the internet, as well as coverage of an evaluation of cloud computing's existing features, service models, and benefits and drawbacks of using cloud computing in social networks.

Table 1: Integrated Compression–Encryption Framework for Social Chatting System

S. No.	Component	Technique / Algorithm	Purpose	Outcome / Benefit
1	Social Chat Input	Text / Audio / Image Data	User communication	Raw data generation
2	Data Preprocessing	Formatting & Segmentation	Prepare data for compression	Reduced redundancy
3	Compression	Huffman Coding / Run-Length Encoding (Lossless)	Reduce message size	Lower bandwidth usage
4	Key Exchange	Elliptic Curve Diffie–Hellman (ECDH)	Secure shared key generation	End-to-end security
5	Text Encryption	AES (Symmetric Encryption)	Confidentiality of text chats	Strong security
6	Media Encryption	RC4	Fast encryption for audio/image	Low computational overhead
7	Transmission	Cloud-based Server	Message delivery	Secure cloud storage
8	Decryption	AES / RC4	Restore original data	Integrity maintained
9	Decompression	Lossless Decompression	Recover original message	No data loss
10	Performance Evaluation	Compression Ratio, Latency, Security	System validation	Improved efficiency

7. SCOPE OF RESEARCH

On a number of different mobile platforms, the suggested application was tested. The following is a summary of some conclusions that may be drawn based on the findings that were collected. End-to-End A key pair is generated using ECDH key exchange and then transferred back and forth between the two parties in order to create the safe shared key that will be used as the key for the encryption techniques. This is how End-to-End Encryption is accomplished. Confidentiality, privacy, and integrity are all ensured by the secure chatting application that has been suggested. Users have the ability to ensure that their communications are inaccessible to everyone, even the company that hosts the service. The data that was sent is only saved in one place, namely the server; none of it is kept on the phone's local storage at any point. The Advanced Encryption Standard (AES) is the method that is used to encrypt text communications. Although it is slower than other block cyphers, it offers a better level of security. The RC4 algorithm is used in the process of encrypting audio and picture communications. This algorithm is among the quickest encryption methods available, and it is appropriate for usage on mobile devices in the process of encrypting incalculable amounts of data.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages 6635-6638

The smartphones and tablets of today are multipurpose gadgets that may also be used for communication. They are portable computers that are worn on the hip and have more memory and can handle more power than portable computers used to just a few of years ago. They are an integral part of our everyday lives and routines. However, additional security concerns arise as a result of the exposure of sensitive information brought about by smartphones and tablets. The most popular types of mobile applications among users are those that facilitate online communication, particularly via the usage of instant messaging. In the world of the internet, governments and other bad people are always striving to hack the servers in order to divulge information about the individuals that use this kind of programme. Mobile chat applications abound in app stores, each with its own unique set of features. A significant number of these programmes make the claim that they protect the information of their users in terms of both its confidentiality and its integrity. The evidence gained via hacking, however, demonstrates that the majority of application developers do not prioritise application security while designing their software.

REFERENCES

M. E. Alex and R. Kishore, "Forensics framework for cloud computing," Comput. Electr. Eng., vol. 60, pp. 193–205, 2017, doi: 10.1016/j.compeleceng.2017.02.006.

N. P. Smart and F. Vercauteren, "Public Key Cryptography – PKC 2010," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6056, pp. 420–443, 2010, [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-79955532534&partnerID=tZOtx3y1.

D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-Trust-a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds," IEEE Trans. Cloud Comput., vol. 5, no. 3, pp. 523–536, 2017, doi: 10.1109/TCC.2015.2415794.

E. G. Bertogna, F. M. Machado, and M. A. Sovierzoski, "An optimized ECG android system using data compression scheme for cloud storage," Health Technol. (Berl)., vol. 10, no. 5, pp. 1163–1171, 2020, doi: 10.1007/s12553-020-00464-z.

Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Commun. Surv. Tutorials, vol. 15, no. 2, pp. 843–859, 2013, doi: 10.1109/SURV.2012.060912.00182.

R. Mathur, V. Pathak, and D. Bandil, "Emerging Trends in Expert Applications and Security," Emerg. Trends Expert Appl. Secur., vol. 841, pp. 357–363, 2019, doi: 10.1007/978-981-13-2285-3.

H. Jung and L. Zhu, "Message from the DIIK 2013 session chairs," Lect. Notes Electr. Eng., vol. 276 LNEE, 2014, doi: 10.1007/978-3-642-40861-8.

B. S. Rawal, "Proxy re-encryption architect for storing and sharing of cloud contents," Int. J. Parallel, Emergent Distrib. Syst., vol. 35, no. 3, pp. 219–235, 2020, doi: 10.1080/17445760.2018.1439491.

Lanani Sadok; Kazar Okba; Hamida Souraya; Wided Oueslati, "BPM approach (business process management) by composition of applications in the cloud computing," 2017 8th International Conference on Information Technology (ICIT), DOI: 10.1109/ICITECH.2017.8079992.

S. Amamou, Z. Trifa, and M. Khmakhem, "Data protection in cloud computing: A Survey of the State-of-Art," Procedia Comput. Sci., vol. 159, pp. 155–161, 2019, doi: 10.1016/j.procs.2019.09.170.

T. Srisooksai, K. Keamarungsi, P. Lamsrichan, and K. Araki, "Practical data compression in wireless sensor networks: A survey," J. Netw. Comput. Appl., vol. 35, no. 1, pp. 37–59, 2012, doi: 10.1016/j.jnca.2011.03.001.

B. Batrinca and P. C. Treleaven, "Social media analytics: a survey of techniques, tools and platforms," AI Soc., vol. 30, no. 1, pp. 89–116, 2015, doi: 10.1007/s00146-014-0549-4.

H. Cui and R. H. Deng, "Revocable and Decentralized Attribute-Based Encryption," Comput. J., vol. 59, no. 8, pp. 1220–1235, 2016, doi: 10.1093/comjnl/bxw007.

H. Cui, R. H. Deng, Y. Li, and B. Qin, "Server-aided revocable attribute-based encryption," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9879 LNCS, pp. 570–587, 2016, doi: 10.1007/978-3-319-45741-3_29.

Q. Dong, Z. Guan, L. Wu, and Z. Chen, "Fuzzy keyword search over encrypted data in the public key setting," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7923 LNCS, pp. 729–740, 2013, doi: 10.1007/978-3-642-38562-9_74.

J. G. Kolo, S. A. Shanmugam, D. W. G. Lim, L. M. Ang, and K. P. Seng, "An adaptive lossless data compression scheme for wireless sensor networks," J. Sensors, vol. 2012, 2012, doi: 10.1155/2012/539638.

S. Kamara and K. Lauter, "Cryptographic cloud storage," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6054 LNCS, pp. 136–149, 2010, doi: 10.1007/978-3-642-14992-4_13.

Y. Lu and J. Li, "Efficient searchable public key encryption against keyword guessing attacks for cloud-based EMR systems," Cluster Comput., vol. 22, no. 1, pp. 285–299, 2019, doi: 10.1007/s10586-018-2855-y.

I. Agudo, D. Nuñez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis, "Cryptography goes to the cloud," Commun. Comput. Inf. Sci., vol. 187 CCIS, pp. 190–197, 2011, doi: 10.1007/978-3-642-22365-5_23.

K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," J. Big Data, vol. 5, no. 1, pp. 1–18, 2018, doi: 10.1186/s40537-017-0110-7.

Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, "Attribute-based Encryption for Cloud Computing Access Control: A Survey," ACM Comput. Surv., vol. 53, no. 4, 2020, doi: 10.1145/3398036.

T. Srisooksai, K. Keamarungsi, P. Lamsrichan, and K. Araki, "Practical data compression in wireless sensor networks: A survey," J. Netw. Comput. Appl., vol. 35, no. 1, pp. 37–59, 2012, doi: 10.1016/j.jnca.2011.03.001.

Z. Tari, "Security and Privacy in Cloud Computing," IEEE Cloud Comput., vol. 1, no. 1, pp. 54–57, 2014, doi: 10.1109/MCC.2014.20.

B. R. Stojkoska and Z. Nikolovski, "Data compression for energy efficient IoT solutions," 2017 25th Telecommun. Forum, TELFOR 2017 - Proc., vol. 2017-January, pp. 1–4, 2018, doi: 10.1109/TELFOR.2017.8249368.

E. G. Bertogna, F. M. Machado, and M. A. Sovierzoski, "An optimized ECG android system using data compression scheme for cloud storage," Health Technol. (Berl)., vol. 10, no. 5, pp. 1163–1171, 2020, doi: 10.1007/s12553-020-00464-z.

R. Mathur, V. Pathak, and D. Bandil, "Emerging Trends in Expert Applications and Security," Emerg. Trends Expert Appl. Secur., vol. 841, pp. 357–363, 2019, doi: 10.1007/978-981-13-2285-3.