Secure Conversation and Images Using End-to-End Encryption on Android in WhatsApp

Amritha R[1], Anu Priya R[2], Initha G[3], Sindhu Priya S[4]

[1]Department of Information Technology, DR NGP Institute Of Technology, Coimbatore, India
amritharavikumar.it[at]gmail.com
[2]Department of Information Technology, DR NGP Institute Of Technology, Coimbatore, India
anupriyaabiseetha007[at]gmail.com
[3]Department of Information Technology, DR NGP Institute Of Technology, Coimbatore, India
inima1621[at]gmail.com
[4]Department of Information Technology, DR NGP Institute Of Technology, Coimbatore, India
sindhusiva52[at]gmail.com

Abstract: ***WhatsApp application have become one of the most important and popular application on smartphones. It has the capability of exchange text messages, images and files for the users to communicate with each other. All messages must be protected. A major issue that is overlooked by most of the people in the instant messaging world is Privacy. Though different Instant Messaging Applications offer different security to users they tend to fail and lead to increase in vulnerabilities and risks of attack on data. Not only business conversations, even in normal conversations our data must be secured, because, anyone's data is very sensitive & data security is highly important to prevent unwanted data losses. To overcome these kinds of vulnerabilities & risks involving attack on data we need an encrypted messaging protocol for a secured conversation. The aim of this paper is securing WhatsApp conversation from targeted advertising and promotion. Increasing the privacy through in-device encryption technique.***

Keywords: Cryptography, Secure Transmission, Encryption, Authentication Server

1. Introduction

Information privacy, or data privacy (or data protection), is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues may arise in response to information from a wide range of sources. Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express them selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information. Privacy may also take the form of bodily integrity.

1. 1 Terms and Terminologies

Data

Data are any facts, numbers, or text that can be processed by a computer. Today, organizations are accumulating vast and growing amounts of data in different formats and different databases. This includes:

- Operational or transactional data - such as, sales, cost, inventory, payroll, and accounting
- Non-operational data - such as industry sales, forecast data, and macroeconomic data
- Meta data - data about the data itself, such as logical database design or data dictionary definitions

Information

The patterns, associations, or relationships among all this data can provide information. For example, analysis of retail point of sale transaction data can yield information on which products are selling and when.

Knowledge

Information can be converted into knowledge about historical patterns and future trends. For example, summary information on retail supermarket sales can be analyzed in light of promotional efforts to provide knowledge of consumer buying behavior. Thus, a manufacturer or retailer could determine which items are most susceptible to promotional efforts.

1.2 How Does Data Security Work

As heterogeneous information systems with differing privacy rules are interconnected and information is shared, policy appliances will be required to reconcile, enforce, and monitor an increasing amount of privacy policy rules (and laws). There are two categories of technology to address privacy protection in commercial IT systems: communication and enforcement.

Policy communication: P3P – The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

Policy enforcement: XACML – The Extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.

EPAL – The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.

WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

Protecting privacy on the internet: On the internet many users give away a lot of information about themselves: unencrypted e-mails can be read by the administrators of an e-mail server, if the connection is not encrypted (no HTTPS), andalso the internet service provider and other parties sniffing the network traffic of that connection are able to know the contents. The same applies to any kind of traffic generated on the Internet, including web browsing, instant messaging, and others. In order not to give away too much personal information, e-mails can be encrypted and browsing of webpages as well as other online activities can be done traceless via anonymizers, or by open source distributed anonymizers, so-called mix networks. Well known open source mix nets include I2P – The Anonymous Network and Tor.

Improving privacy through individualization: Computer privacy can be improved through individualization. Currently security messages are designed for the "average user", i.e. the same message for everyone. Researchers have posited that individualized messages and security "nudges", crafted based on users' individual differences and personality traits, can be used to further improve each person's compliance with computer security and privacy.

1.3 Risk Management

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (manmade or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk."

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

Research has shown that the most vulnerable point in most information systems is the human user, operator, designer, or other human process.

In broad terms, the risk management process consists of:

- Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
- Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
- Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
- Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
- Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.

Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost-effective protection without discernible loss of productivity. For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.

1.4 Security Controls

Selecting and implementing proper security controls will initially help an organization bring down risk to acceptable levels. Control selection should follow and should be based on the risk assessment. Controls can vary in nature, but fundamentally they are ways of protecting the confidentiality, integrity or availability of information. Organizations can implement additional controls according to requirement of the organization.

Administrative

Administrative controls consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day-to-day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed –

the Payment Card Industry Data Security Standard (PCI DSS) required by Visa and MasterCard is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls, which are of paramount importance.

Logical

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. Passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption are examples of logical controls.

An important logical control that is frequently overlooked is the principle of least privilege, which requires that an individual, program or system process not be granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read email and surf the web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, employees are promoted to a new position, or employees are transferred to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges, which may no longer be necessary or appropriate.

Physical

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities and include doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and workplace into functional areas are also physical controls.

An important physical control that is frequently overlooked is separation of duties, which ensures that an individual cannot complete a critical task by himself. For example, an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator; these roles and responsibilities must be separated from one another.

Cryptography:

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage. Cryptography provides information security with other useful applications as well, including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older, less secure applications such as Telnet and File Transfer Protocol (FTP) are slowly being replaced with more secure applications such as Secure Shell (SSH) that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry-accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure (PKI) solutions address many of the problems that surround key management.

1.5 Change Management

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made.

Any change to the information processing environment introduces an element of risk. Even apparently simple changes can have unexpected effects. One of management's many responsibilities is the management of risk. Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they may disrupt critical business processes or interfere with other changes being implemented.

Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying a new desktop computer are examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk to the processing environment and are not a normal everyday activity. The critical first steps in change management are (a) defining change (and communicating that definition) and (b) defining the scope of the change system.

Change management is usually overseen by a change review board composed of representatives from key business areas, security, networking, systems administrators, database administration, application developers, desktop support and the help desk. The tasks of the change review board can be facilitated with the use of automated work flow application. The responsibility of the change review board is to ensure the organization's documented change management procedures are followed. The change management process is as follows

Request: Anyone can request a change. The person making the change request may or may not be the same person that performs the analysis or implements the change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organizations business model and practices, and to determine the amount of resources needed to implement the change.

Approve: Management runs the business and controls the allocation of resources therefore, management must approve requests for changes and assign a priority for every change. Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices. Management might also choose to reject a change request if the change requires more resources than can be allocated for the change.

Plan: Planning a change involves discovering the scope and impact of the proposed change, analyzing the complexity of the change; allocation of resources and, developing, testing and documenting both implementation and back-out plans. Need to define the criteria on which a decision to back out will be made.

Test: Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment. The back out plan must also be tested.

Schedule: Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.

Communicate: Once a change has been scheduled it must be communicated. The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the help desk and users aware that a change is about to occur. Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.

Implement: At the appointed date and time, the changes must be implemented. Part of the planning process was to develop an implementation plan, testing plan and, a back out plan. If the implementation of the change should fail or, the post implementation testing fails or, other "drop dead" criteria have been met, the back out plan should be implemented.

Document: All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.

Post-change review: The change review board should hold a post-implementation review of changes. It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement.

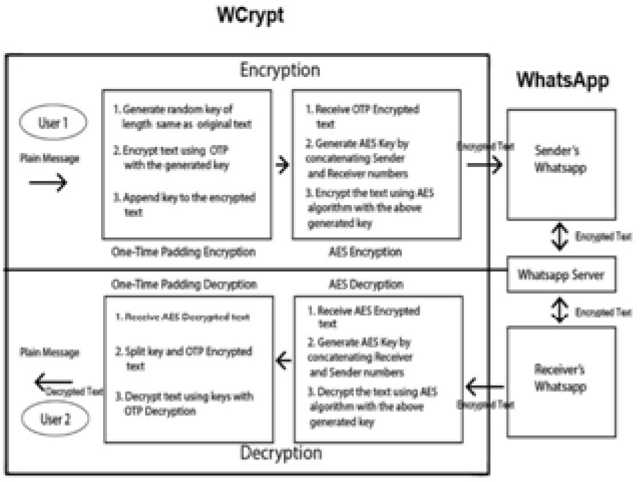
Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment. Good change management procedures improve the overall quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication.

1.6 Advantages of Data Security

- Protect networks, computers and data from unauthorized access
- **Protection of Valuable Information –** Information is one of the most valuable assets of any enterprise. Its protection is an important part of IT infrastructure. Integrating security solution can protect all information.
- **Keeping Ahead of Competitors –** Implementing Security Solutions keeps organization ahead in competition. IT Security Solution fits into existing business processes. Data protection acts as icing on the cake.
- It generates a good image and reputation. Improved stakeholder confidence in your information security arrangements.
- Faster recovery times in the event of disruption. It ensures the continuity of critical business operations in the event of natural disasters or high-impact security incidents
- It ensures compliance with laws and regulations. Improved company credentials with the correct security controls in place.

2. System Design

2.1 Overview of Architecture


WCrypt
Encryption
WhatsApp
User 1
Plain Message
1. Generate random key of length same as original text
2. Encrypt text using OTP with the generated key
3. Append key to the encrypted text
One-Time Padding Encryption
1. Receive OTP Encrypted text
2. Generate AES Key by concatenating Sender and Receiver numbers
3. Encrypt the text using AES algorithm with the above generated key
AES Encryption
Encrypted Text
Sender's Whatsapp
Encrypted Text
Whatsapp Server
Encrypted Text
Receiver's Whatsapp
Encrypted Text
One-Time Padding Decryption
AES Decryption
1. Receive AES Decrypted text
2. Split key and OTP Encrypted text
3. Decrypt text using keys with OTP Decryption
1. Receive AES Encrypted text
2. Generate AES Key by concatenating Receiver and Sender numbers
3. Decrypt the text using AES algorithm with the above generated key
Plain Message
Decrypted Text
User 2
Decryption

3. Proposed System

The WCrypt uses multiple encryption algorithms to secure chats. One Time Pad (OTP) Algorithm and AES algorithm is used for encryption. The encrypted text is then encrypted again using AES algorithm with a key which is generated by hashing sender and receiver number using SHA256 algorithm. The proposed system does not require internet connection, thus making it more secure and ensuring original text is not saved anywhere, preventing any kind of mining.

3.1 Read Contacts

A contact list is a collection of screen names. It is a commonplace feature of instant messaging, Email clients, online games and mobile phones. It has various trademarked and proprietary names in different contexts.

The contact list is just a list. Its window shows screen names that represent actual other people. To communicate with someone on the list, the user can select a name and act upon it, for example open a new E-mail editing session, instant message, or telephone call. In some programs, if your contact list shows someone, their list will show yours. Contact lists for mobile operating systems are often shared among several mobile applications.

Contact list is filtered and is used to initiate conversation by picking up a particular contact available on WhatsApp messenger.

3.2 Text Encryption

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm – a cipher – generating ciphertext that can be read only if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature. Standards for cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem.

3.3 Transmit Encrypted Text

A point-to-point message transmission is a communications medium with exactly two endpoints and no data or packet formatting. The host computers at either end take full responsibility for encrypting and decrypting the data transmitted between them. The connection between the sender and receiver involves a communication medium and the communications medium used here is WhatsApp.

3.4 Text Decryption

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

3.5 Store Decrypted Text

SQLite is a relational database management system contained in a C programming library. In contrast to many other database management systems, SQLite is not a client–server database engine. Rather, it is embedded into the end program.

SQLite is ACID-compliant and implements most of the SQL standard, using a dynamically and weakly typed SQL syntax that does not guarantee the domain integrity.

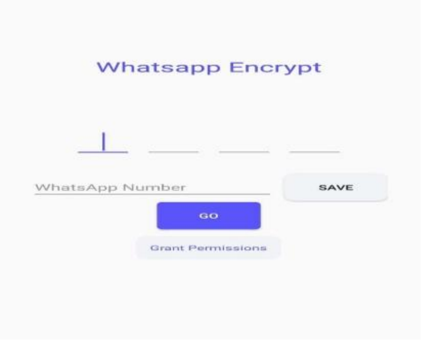
SQLite is a popular choice as embedded database software for local/client storage in application software such as web browsers. It is arguably the most widely deployed database engine, as it is used today by several widespread browsers, operating systems, and embedded systems (such as mobile phones), among others. SQLite has bindings to many programming languages.

3.6 Display Conversation

The RecyclerView is a new ViewGroup that is prepared to render any adapter based view in a similar way. It is supposed to be the successor of ListView and GridView, and it can be found in the latest support-v7 version. One of the reasons is that RecyclerView has a more extensible framework, especially since it provides the ability to implement both horizontal and vertical layouts. Use the RecyclerView widget when you have data collections whose elements change at runtime based on user action or network events.

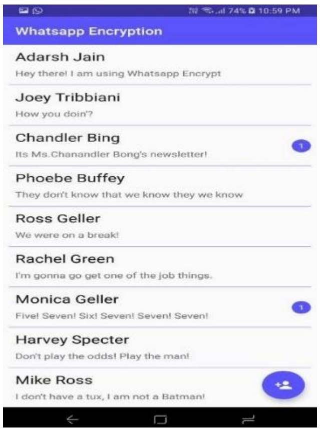
4. Application Opening Screen

- Enter your phone number which is connected with WhatsApp.
- Click and save your number.
- Enter your security code, to proceed to the application.



All Chats Screen:

- Displays all the chats with the corresponding contact name.
- On clicking a particular contact name, the chat screen of the corresponding chat is displayed.
- The add new chat button below displays all the contacts available to start a new chat.



74% 10:59 PM

Whatsapp Encryption

Adarsh Jain
Hey there! I am using Whatsapp Encrypt

Joey Tribbiani
How you doin'?

Chandler Bing
Its Ms.Chanandler Bong's newsletter!

Phoebe Buffey
They don't know that we know they we know

Ross Geller
We were on a break!

Rachel Green
I'm gonna go get one of the job things.

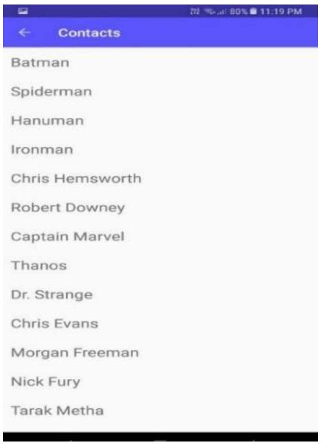
Monica Geller
Five! Seven! Six! Seven! Seven! Seven!

Harvey Specter
Don't play the odds! Play the man!

Mike Ross
I don't have a tux, I am not a Batman!

Add New Contact

- Displays all the contacts available in the phone.
- On clicking a particular contact, it initiates a chat with the contact enabling encryption.



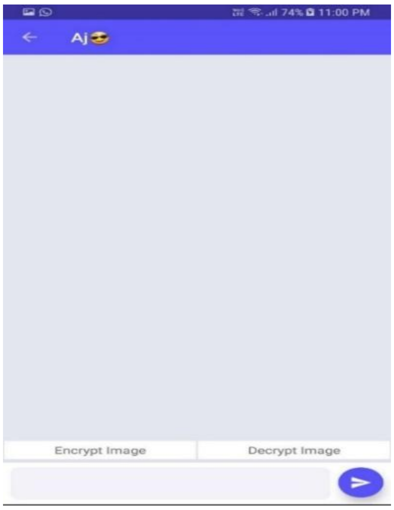
80% 11:19 PM

Contacts

Batman
Spiderman
Hanuman
Ironman
Chris Hemsworth
Robert Downey
Captain Marvel
Thanos
Dr. Strange
Chris Evans
Morgan Freeman
Nick Fury
Tarak Metha

Chat Screen

- It is the interface displaying the messages sent and received between two people.
- Clicking the text box allows us to type and send a message.
- Encrypt/ Decrypt Image button allows encrypted media exchange.



5. Conclusion

Encryption technology, however, is revolutionizing the way communication is performed on daily basis. This technology makes it possible for users to maintain their privacy and communicate without the fear of someone eavesdropping their conversation. For instant messaging, this means that sharing private information, communicating without worrying on privacy issues and sharing of sensitive information can all be done simply through an app on your mobile devices.

Acknowledgement

We express our hearty thanks to our project guide, **Mrs. M. Sreerajeswari,** Assistant Professor, Department of Information Technology, for his valuable guidance and timely help for completing our project.

References

[1] Minta Thomas, Panchami V. "An Encryption Protocol for End-to-end Secure Transmission of SMS". 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT].

[2] Punam Milind Chabukswar, Manoj Kumar, P. Balaramudu. " An Efficient Implementation of Enhanced Key Generation Technique in Data Encryption Standard (DES)Algorithm using VHDL". Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).

[3] Edward L. Witzke, Lyndon G. Pierson."Key Management for Large Scale End-toEnd Encryption".

[4] Marko Hassinen.SafeSMS - "End-to-end encryption for SMS messages".8th International Conference on Telecommunications .

[5] Mohamed Nabeel. "The Many Faces of End-to-End Encryption and Their Security Analysis". 2017 IEEE 1st International Conference on Edge Computing.

[6] Ammar Hammad Ali, Ali MakkiSagheer"Design of Secure Chatting Application With End To End Encryption For Android Platform". 2017 Iraqi Journal for Computer and Informatics.

[7] Sarita Kumari "A Research Paper on Cryptography Encryption and Compression Techniques". 2017 International Journal Of Engineering And Computer Science.

[8] KadhimH.K.Alibreheemi, Wafaa A.A. Alrekaby"Design and Implementation Encrypted Call Application on Android System".2015 International Journal Of Computer Science and Mobile Computing.

[9] Noor Sabah, Jamal M. Kadhik and Ban N. Dhannoon "Developing an End-to-End Secure Chat Application".2017 IJCSNS International Journal of Computer Science and Network Security.

[10] Monika Agarwal, "A Comparative Survey on Symmetric Key Encryption Techniques".2012 International Journal on Computer Science and Engineering.

[11] M.Hassinen, "Java based public key infrastructure for SMS messaging".2012 International Conference on IEEE.

[12] Zhang Qing, "Iterative Hashing Algorithm Base on MD5, Journal of Computer Science Engineering 2011.

[13] Monika Agrawal, A Comparative Survey on Symmetric Key Encryption Techniques, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012.

[14] William Stallings, Cryptography and Network Security Principles and Practices Fourth Edition.

[15] Ketu File white papers, Symmetric vs Asymmetric Encryption, a division of Midwest Research Corporation.

[16] M. Hassinen, Java based public key infrastructure for SMS messaging, in Proc. 2nd ICTTA, 2006, pp. 8893.

[17] S. Wu and C. Tan, A high security framework for SMS, in Proc. 2nd Int. Conf. BMEI, 2009, pp. 16.

[18] A. De Santis, G.Cattaneo, M. Cembalo, F. Petagna, and U. F. Petrillo, An extensible framework for efficient secure SMS, in Proc. Int. Conf. CISIS, 2010, pp. 843850.

[19] J. L.-C. Lo, J. Bishop, and J. H. P. Eloff, SMSSec: An end-to-end protocol for secure SMS, Computer Security, vol. 27, nos. 56, pp. 154167, 2008. [8] M. Toorani and A. Shirazi, SSMS: A secure SMS messaging protocol for the m-payment systems, in Proc. IEEE ISCC, Jul. 2008, pp. 700705.

[20] TingyuanNie, Chuanwang Song, XulongZhi, Performance Evaluation of DES and Blowfish Algorithms, IEEE, 2010.

[21] Diaa Salama Abdul Minaam, Hatem M. AbdualKader, and Mohiy Mohamed Hadhoud, Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types, International Journal of Network Security, Vol.11, No.2, PP.7887, Sept. 2010.

[22] Najib A. Kofahi, Turki Al-Somani and Khalid Ai-Zamil, Performance Evaluation of Three Encryption/Decryption Algorithms, IEEE, 2010.

[23] DiaaSalama, HatemAbdual Kader, and MohiyHadhoud, Wireless Network Security Still Has no Clothes, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012