Digital Signature Authentication and Verification on Smart Phones using CRιPT Algorithm

Aishwarya Mali[1], Chinmay Mahalle[2], Mihir Kulkarni[3], Tejas Nangude[4], Prof. Geeta Navale[5]

[1234] *Final Year Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*

[5] *Project Guide, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India*

---***---

Abstract - *With the use of mobile devices as a client for internet, the threat of unauthorized and unauthenticated access of crucial documents (e.g.: contracts, bonds, receipts, etc.) is increasing day by day. Although Digital Signature is meant to be the solution for the unauthorized access, its implementation is not adequate till now. Symmetric data transfer mechanism is used for the transfer of important documents, but there is a need of more competent mechanism for safe transfer and verification of the documents. Here we contemplate a RESTful service as well as Jersey Framework enabled data transfer mechanism for the transfer of document using Smart Phones. We have suggested the design of CRiPT (Cipher using Random Integer Procreation and Translation) Algorithm in this paper. CRiPT algorithm not only defines effective cryptography but is also light weighed; thus effective for smart-phones. Cryptography concepts – Random number generation, have been used to develop an encryption-decryption algorithm to obtain a ciphered Digital Signature for security purposes. Use of Digital Signature resolves the Document Authentication issue. A Hash-value based verification process is defined to ensure that an authenticated sender has only sent the document to intended recipient. The main aim is to tackle issues related to digital document transfer over the network, by making the overall process handy using Smart phones as well as ensuring Information Security.*

Key Words*:* *Digital Signature, RESTful service, Jersey Framework, Cryptography, Random number generation, Authentication, Verification, Information Security***.**

1.INTRODUCTION

Smartphones are being used on a great scale now-a-days. Many daily activities depend on it, making it a very integral part of life. It might contain a lot of private information such as pictures, passwords, call logs, messages, etc. of the user. This information is highly vulnerable if at all smartphone is stolen or borrowed. Also, this includes sending document over the internet through smartphones. Some documents might be highly confidential and require a high level of security while transferring because of the threat of document being intercepted. This can be done using technique known as cryptography. If a digitally signed document is sent over internet, the sent document and the received document both are genuine. Cryptography is a method of storing and transmitting data in a particular form so that only for those it is contemplated can read or process it. This can be done effectively in smartphones. It is the method of encoding the content so that for whom it is intended only can read it. Digital signature is a code which is generated by public key encryption and is used to authenticate and verify the document sent over a network. It is also used to verify the sender's identity.

Today digital signatures are being used in many different forms. Some use a literal signature of a person on screen and detect it using image processing techniques. This is not very reliable process as handmade signature might slightly differ from each other and result in forbidden access. Also another way is carrying a small USB device containing our digital signature and connecting the device to system to embed the digital signature. The limitation for this is that our signature totally depends upon the device we carry with us. If the device itself is stolen or misplaced, we might land up in trouble. Moreover, the device is expensive. The most secured way for implementation of digital signatures considered on this date is biometric signatures. But again, all the smartphones are not provided with biometric security systems. So in this paper we present a cost effective, simple, accurate, highly secured Digital Signature authentication and verification technique using smartphones.

There are different survey papers that cover different aspects of the cryptography technology. For example, in [7] we study about the existing techniques developed using cryptography. Also the advantages and disadvantages of these techniques are seen here. In [2], we see how a low cost digital signature can be developed and can anomalous behavior in the system be identified. Moreover, paper [3] shows us technique to use digital signature architecture that can be used for web-based application. And paper [1] tells us what the existing methods of using digital signatures are in mobile device systems.

The rest of the paper is organized as follows: Section II provides the literature survey of referred papers. Section III includes architecture diagram, methodology and algorithm of the proposed system. Section IV provides comparison with RSA algorithm. In section V we present different advantages and constraints of the proposed system. Conclusion and Future scope is presented in sections VI and VII respectively. Acknowledgement to external as well as internal guide is presented in section VIII, whereas section IX includes references.

2. STATE OF THE ART

Internet and mobile devices becoming the basic amenities of livelihood, there is a dire need for maintaining privacy. [1] enlightens the necessity by integrating the digital signature schemes with the mobile applications which we access on regular basis, such as to play games, receive emails, purchase books, etc. The approach proposed here is named as Server based Signature (SBS), which happens to be very useful for mobile communication systems.

Main advantage covered in [1] is reduction of computation complexity on mobile devices. Other advantages are reduction of communication consumption between signer and verifier and achieve same security level as that of traditional Digital Signature protocols.

[2] aims to use the data streams generated by the log files based on the user's location, call log, message logs etc and verify whether the individual using the smart phone is the authenticated user or not. In this paper the sensor based data stream generation is replaced by the log files which are previously generated automatically.

The traditional way of securing the data is rejected and new techniques of data security are presented. Also the verification of the user is done using the data stream generated based on the log files, so there is no need of explicitly embedding sensors to generate the data streams. Verification is done based on different aspects such as location, call logs (Call duration and individual called), message log (Messages sent and replied), indoor and outdoor mobility. The use of the explicit sensors is avoided so the battery life of the device will not get affected. The Power consumption of the SALCS based model is less than that of GPS based model. It is the cost effective technique of verification of the user and hence maintain integrity of data.

In today's competitive business world, in which enterprises must extend their business environments over the Web for consumers, employees, and partners, digital security plays a vital role in building trust and credibility. Paper [3] highlights on a digital signature architecture that provides browser-agnostic, client-side signature components and generic server-side signature validation components to help integrate signatures into Web applications. The approach proposed in this paper is *Java-Based Digital Signature architecture for Web-apps.* The configuration repository is a centralized store for all configuration parameters and is the key component for a centralized, parameter-driven architecture. *Certificate and CRL repository:* This component is mainly responsible for organized storage of certificates and CRLs, which are required for successful certificate status validation. *Secure Private Key Storage:* This component abstracts the details of underlying private key storage and format. It provides a rational interface to access and manage private keys securely for signing.

The main aim of [4] is to present reliable technique of authentication using Digital Signature so that users can authenticate the document at any time, at any place using various platforms including laptop, desktop, web portals, mobile devices etc. In this technique there is no need of explicitly using third party software for the authentication of the digital signature. [4] presents a Digital Signature technique in which the signature will not be stored on any server instead it will be regenerated whenever needed. This regeneration of the signature will be based on the JavaScript program, which will be downloaded in the backend when the key regeneration process is initiated.

Paper [5] suggests secure transfer of image over the network. The image which is being transferred should be authorized and authenticated. The proposed solution includes the use of different algorithms. The algorithms are *SHA1* for hash generation, *Reed Solomon* algorithm for transmission and storage of digital data, the *RSA* algorithm for generation of the Digital Signature and *Chaotic map* for different operations. The simple method is that first the hash of the image is generated using the SHA1 algorithm, then using the RSA algorithm the digital signature is generated.

Paper [6] proposes a method for contract signing which can be approved with Signer Identity Card. Users first have to register for using the application. The authentication of the user is done before accessing the contract. Also the signing of the contract is made easy.

In the method suggested in [6], the system uses National identity card to assign a unique user identity. But there might be a possibility of misuse of a card by any other person who may use this card to access the document and manipulate it.

The Man-in-the-Middle attack is one of the biggest concerns in the security professionals, which targets the actual data between the end points and disrupts the integrity and security of the system. The paper represents the survey of the Man-in-the-Middle attack in brief. The comparison of different scenarios in man-in-the-middle attack is given in [9]. Paper [10] aims to find different techniques of man-in-the-middle attack on the HTTPS network and classify these techniques to make the HTTPS network stronger and intrusion free. Man-in-the-middle attack is capable of breaking the security of the Hyper Text Transfer Protocol Secure. The main intension of [10] is to study different scenarios in which the man-in-the-middle attack is possible and prepare a framework which will be able to classify the man-in-the-middle attacks in the HTTPS network.

Nowadays password based authentication is used to authenticate the user for a particular system. Unique User ID and password is given to the user for authentication purpose. Web based application using this system can be target of brute force attack. In [11] a simple, practical and secure system is proposed. This system is non-intrusive and can be used to secure web applications.

3. PROPOSED SYSTEM

The proposed system is capable of sending the document with an embedded Digital Signature so that the receiver is sure that the document he has received is 100% authentic. Also the system checks if the sender sending the document is really the person whose account is being used. There is a login mechanism for first step of user authentication. After this, clause mechanism is implemented which will be discussed later in the chapter. Document will be transferred along with the hash value and ciphered random numbers for verification purpose.

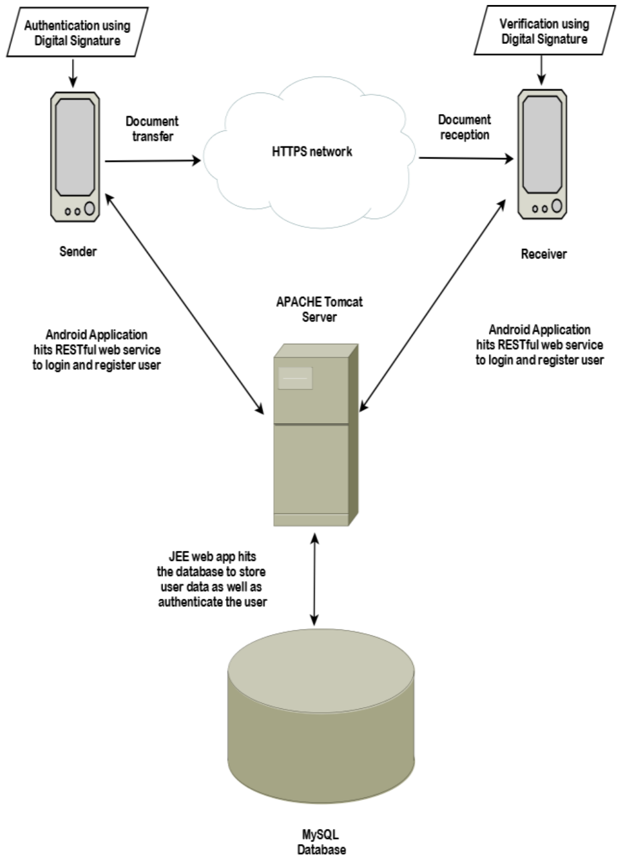
Authentication using Digital Signature
Verification using Digital Signature
Document transfer
HTTPS network
Document reception
Sender
Receiver
APACHE Tomcat Server
Android Application hits RESTful web service to login and register user
Android Application hits RESTful web service to login and register user
JEE web app hits the database to store user data as well as authenticate the user
MySQL Database

Figure 3.1: System Architecture

The flow of the system is as follows:

1. Users (sender and receiver) register themselves after installing application on their smart phones.
2. User details along with encrypted digital signature and mapped clause numbers would be stored in database.
3. The sender will browse his phone for the required document to be sent and attach it.
4. Sender will enter required receiver details and enter the proper combination of sentence when asked, for authentication purpose.
5. Receiver will receive a document along with an unrecognizable hash value appearing on the screen.
6. Receiver's phone will also receive inputs for decryption algorithm and will verify if the document sent is authentic.

This is the overview of the implementation of the proposed system. Let us see each step in detail.

Registration

Here, the sender and the receiver will enter all the required details of themselves if they are using the application for the first time. Option to register is provided on the login screen (main activity) of the application. Details asked in the registration process are:

- **Username**: Should be at least 5 characters long
- Password: Should be at least 8 characters long and alphanumeric
- **Email ID**: Proper format to be followed; e.g. "abc@example.com"
- **First name** and **last name**
- **Digital signature**: Should be 4 characters long and should only consist of small letters (capital letters, numbers & special symbols are not allowed).
- **Security question**: Select a question of which only you know the answer.
- **Answer**: Set a suitable answer for the selected security question. This will be used in case you forget your password.
- **Clauses**: Select one part of the sentence from each of the three given spinners which will form a meaningful sentence. Remember this sentence formation as it will be asked to user before sending and receiving the document.

Database

The information entered will be stored in database through RESTful API. Database used is MySQL. Digital Signature will be stored in database in its encrypted integer format. This database is accessed by the phone from time to time for various purposes like checking user credentials while logging in, digital signature retrieval, checking for the correct order sentence and verification.

File Exploring and Attaching

The file to be sent over the network should be present in the internal or extended storage of the device. When the user successfully logs into his account, he is asked to browse the file. After navigating to the file to be sent, it is attached.

Document Transfer

Before sending the document, sender first of all needs to enter the required details of the receiver. Then the sender is asked to enter the combination of the sentence in 3 spinners provided. Note that the sentence formed should be the same sentence he chose while registering himself. This ensures that the person sending the document is legitimate. Along with document the hash value generated and encrypted random numbers used in the process are also sent.

Verification Process

Now the document is received at the receiver's end. Program has a hash value sent by the sender. This hash value is decrypted using same random numbers used to generate it. Now, receiver program has an integer number which is compared with the sender's digital signature in database. If it matches, the document sent is authentic.

Received Document

Before the user is allowed to access the document, he needs to go through clause mechanism. It is the same as mentioned in above steps. This is to ensure that the person to whom the file.

CRiPT (**C**ipher **R**andom **i**nteger **P**rocreation and **T**ranslation) **Algorithm** is explained below:

Encryption:

Input: an array containing character digital signature say *a[]* of size *n* = 4.

Function #1: to convert digital signature from string to integer.

- For array index *i* = 0 to 3
    - Replace each character from digital signature by an integer number in the range 21 to 46 corresponding to 'a' to 'z' respectively.
    - Store the replacement in integer array say *b[]* of size *n* = 4.

$$\pi(a[\ ]) = q(b[\ ] \rightarrow xi \in \{21......46\}),$$
$$if\,(p(a[\ ] \rightarrow yi \in \{'a'......'z'\}))$$

#Above step converts the character array into integer array.

- Obtain an integer whole number for integer array using following equation:

$$IntegerSign(\alpha) = b[3] + (b[2] * 10^2) + (b[1] * 10^4)$$
$$+ (b[0] * 10^6)$$

- Return α.

Function #2: to manipulate integer digital signature using random numbers.

- Random1 $r1 \in \{1......45\}$
- $IntermediateValue(\beta) = a * r1$
- Random2 $r2 \in \{1000......9000\}$
- $HashValue(\gamma) = \beta + r2$
- $c[0] = \gamma$
$c[1] = r1$
$c[2] = r2$
- Return *c[]*;

Output: Hash value corresponding to 4 character digital signature is obtained.

Table 3.1: Encryption Algorithm

Input: an array *c []* containing the hashed digital signature.

Algorithm:

- $\gamma = c[0]$
$r1 = c[1]$
$r2 = c[2]$
- $\beta = \gamma - r2$
- $decryptInt(\partial) = \beta \div r1$
- $inTemp4(\rho 4) = \partial \% 10^2$

# Storing 4th number in array

- $b[3] = \rho 4$
- $inTemp3(\rho 3) = \partial \% 10^4$

# Storing 3rd number in array

- $temp3(\sigma 3) = (\rho 3 - \rho 4) \div 10^2$
- $b[2] = \sigma 3$
- $inTemp2(\rho 2) = \partial \% 10^6$

  # Storing 2nd number in array
- $temp2(\sigma 2) = (\rho 2 - \rho 3) \div 10^4$
- $b[1] = \sigma 2$
- $inTemp1(\rho 1) = \partial \% 10^8$

  # Storing 1st number in array
- $temp1(\sigma 1) = (\rho 1 - \rho 2) \div 10^6$
- $b[0] = \sigma 1$
- For array index *i* = 0 to 3
  - Replace integer number 21 to 46 by ‘a’ to ‘z’ respectively (reverse of encryption).
  - Store the replacement in character array *a[]* of size *n* = 4.

$$\pi(b[\ ]) = q(a[\ ] \rightarrow yi \in \{'a'......'z'\}),$$
$$if(p(b[\ ] \rightarrow x1\{21......46\}))$$

- Convert character array into String and store in stringSign (ω)
- Return ω

Output: Digital Signature in original character format of size 4 characters.

Table 3.2: Decryption Algorithm

5. COMPARISON WITH EXISTING TECHINIQUES

Currently there are various techniques and methodologies in market for implementation of digital signatures. Some of the currently used techniques are listed below:

1) Image processing:

- In this technique the user has to actually sign the digital document on the screen using special devices. To verify if the signature is authentic, the sign is compared pixel-to-pixel with the pre-stored sign of the same person in database. If the sign matches up to the threshold percentage, the digital document is considered to be sent by authentic user.
- There are some drawbacks in this system. The accuracy is very fragile and even the authenticated user may fail to verify himself due to human error as the signature may not be the same each time. Also expensive devices are involved like light pen using which the signature is to be embedded on the document.
- The proposed solution tackles these drawbacks as digital signature is in the form of characters. Thus, the human error problem can be solved. Also, no separate devices are needed to be bought to use the application suggested here.

2) Two-factor Authentication:

- Instead of a 1 step verification process, two-factor authentication carries out a 2 step verification process for better security and authentication. Various methods used in this technique are pass-code matching, one-time password, facial recognition, finger-print scanner etc.
- The main problem in this technique is requirement of very high level security, because if the attacker gets the knowledge of even one of the authentication factor, may lead to disaster.
- In proposed system, the generation of hash value is done using random number every time. Thus, the probability of hacking the system reduces dramatically.

3) RSA Algorithm:

- RSA is an asymmetric cryptographic algorithm. RSA algorithm enables the user to create and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret; these prime factors correspond to private key.
- The drawback of RSA algorithm is that security of RSA depends on the computational difficulty of factoring large integers; encryption strength is directly bound to key size. Thus making it difficult to implement on small handheld devices like smart phones as these devices have low computational capacity.
- The proposed algorithm is a light weight algorithm as it avoids creation and transmission of public and private keys and also the complex computations associated with it. Thus making it feasible to be implemented on handheld devices like smart phones.

4) SBS Technique

- Server Based Signature is a proposed system in [1]. In this system, the signature is stored on a server and retrieved whenever required. It is specifically designed so as to be compatible to handheld devices.
- SBS scheme uses one-way collision resistant Hash function which is quite an old technique and at the same time ambiguous in its efficiency. Also, verification process is kept the same as that of Asymmetric Cryptographic Algorithm
- In the proposed system, the algorithm used is unambiguous and only the concept of Asymmetric Cryptographic Algorithm is used and not the actual algorithm.

Comparison with existing techniques in tabular form

Techniques	Attributes			
	Accuracy	**Efficiency for smart-phone**	**Security**	**Simplicity**
Image Processing	Low	Medium	Medium	Low
Two-factor Authentication	Medium	High	Medium	Low
RSA	High	Low	High	Low
SBS	Medium	High	Medium	Medium
CRiPT	High	High	Medium	High

Table 4.1: Comparison with existing techniques

Comparison with existing techniques in graphical form

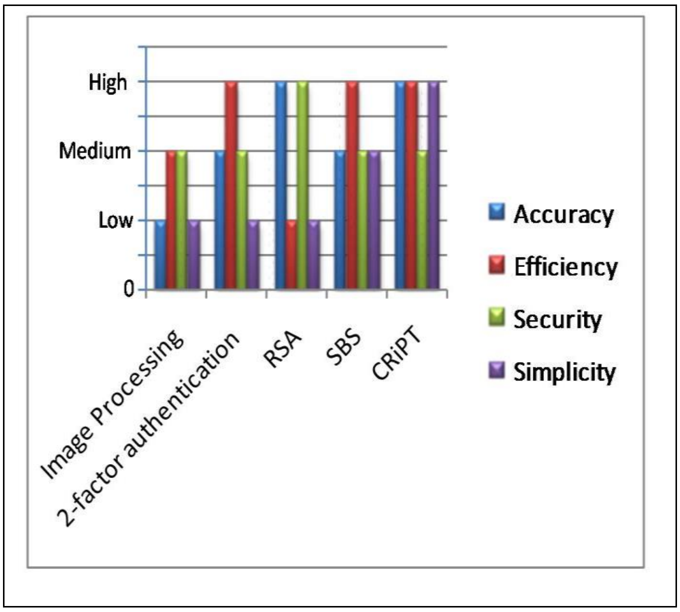

Chart 4.1: Comparison with existing techniques

5. ADVANTAGES AND CONSTRAINTS OF THE PROPOSED SYSTEM

The advantages of the proposed system can be summarized as follows –

- The overall process of attaching Digital Signature to document and transferring it over the network to the intended recipient, is made very handy by the use of smart phones.
- The overall level of information security and data integrity is increased.
- Users can authenticate their documents by attaching Digital Signature to them at anytime from any place, by the use of database.
- The system achieves Information security, Data Integrity, Authenticity and Usability by all means.

The proposed system has following constraints –

- **Language of interaction with the system:**

The Language in which the user will interact with the system is limited to only one language i.e. English. Other language support is not provided. Hence even a general user must know English to use the system.

- **Importing the document:**

The document in which sent over the network, must be necessarily stored in the user's smart phone storage. The document cannot be imported from any other application or not even from cloud storage.

- **Continual smart phone usage by the user:**

The underlying functionality is made available through smart phones only. There is no web portal that supports the system functioning. Hence the only medium of access is the smart phone.

- **No updating/ deleting service for the user account:**

Once the user submits his/her details at the time of registration, they cannot be updated further. Also the user cannot delete any of his details. This has been incorporated to ensure that there is no third party access to user account i.e. nobody else other than the user can access his account by updating any of the details or deleting previous details and creating a new account under the name of the user.

6. CONCLUSION

The project is based on the domain of Information Security where it is intended to secure the data being transferred over the network from any malicious attack as well as ensure its authenticity and integrity. The system works in an action – response manner, where the user, mobile application, server and database interact with each other simultaneously throughout the execution process via RESTful web service. Document security is provided through cryptography algorithms i.e. encryption/decryption and verification process. It is specifically ensured that the system is accessible to only registered and authenticated users. Any type of unauthorized access leads to user abortion from the system. Thus the system is in complete accordance with gathered requirements in the software specification documentation.

7. FUTURE SCOPE

As the use of the internet is increasing day by day, there is a need of Data Authentication and Verification. Digital Signature is one of the solution for these problems. This paper has presented a technique to make digital signature handy and easy to use. Proposed solution is smartphone based that makes the Digital Signature portable. Android platform is used here, which is open source and hence there is huge scope of improvement and advancement. Asymmetric Encryption technique is proposed for the encryption of the Digital Signature which gives a very secure way to verify the authenticity of the data. Also it is very cost efficient technique for the authenticity and verification of data. There is no need of using any explicit device to access a digital signature only the mobile is required which is connected to the network.

ACKNOWLEDGEMENT

This research was supported by **Graphikera Technologies**. We thank Mr. Husain Basrawala, Chief Technology Officer, Graphikera technologies, for all the support throughout the research. Also we would like to express our sincere gratitude towards Prof. Geeta S. Navale, Head of Department, Computer Engineering, Sinhgad Institute of Technology and Science for guiding, assisting and providing her valuable suggestions to us from time to time; that has greatly helped to improve the manuscript.

REFERENCES

[1] Yeu Lei, Deren chen, Zhongding Jiang, “Generating Digital Signature on mobile devices”, 18th International Conference on Advanced Information Networking and Application, 2004.

[2] Senaka Buthpitiya, Anind K. Dey, Martin Griss, “Soft Authentication with Low-Cost Signatures”, 2014 IEEE conference on pervasive computing and communications.

[3] Harigopal K.B. Ponnapalli and Ashutosh Saxena, “A Digital Signature Architecture for Web Apps”, Infosys, India, March/April 2013.

[4] Carlisle Adams and Guy-Vincent Jourdan, “Digital Signatures for Mobile Users”, 2014 IEEE Conference, Toronto, Canada.

[5] Shahzad Alam, Amir Jamil, Ankur Saldhi, Musheer Ahmad , “Digital Image Authentication and Encryption using Digital Signature”, 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) IMS Engineering College, Ghaziabad, India

[6] Emir Husni, Bramanto Leksono , Muhammad Ridho Rosa , “Digital Signature for Contract signing in Service Commerce”,2015 International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E) Samosir Island, North Sumatra, Indonesia, September 7-9, 2015 .

[7] Shivendra singh, Md. Sarfaraz iqbal, Arunima Jaiswal, “Survey on Techniques Developed using Digital Signature: Public key Cryptography,” International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 16, May 2015.

[8] Alpizar-Chacon, Mario Chacon-Rivas, “Authenticity and versioning of learning objects using the digital signature infrastructure of Costa Rica”, 2014.

[9] Mauro Conti, Nicola Dragoni, and Viktor Lesyk , “A Survey of MAN-IN-THE-MIDDLE attacks” 2015 IEEE Communication Surveys & Tutorials.

[10] Shaun Stricot-Tarboton, Sivadon Chaisiri, Ryan K L Ko , “Taxonomy of MAN-IN-THE-MIDDLE attacks on HTTPS”, 2016 IEEE TrustCom-BigDataSE-ISPA .

[11] Carlisle Adams , Guy-Vincent Jourdan , “Lightweight protection against Brute Force Login attacks on Web Applications” 2010 Eighth Annual International Conference on Privacy, Security and Trust.

[12] Santi Jarusombat and Surin Kittitornkun, “Digital Signature on Mobile Devices based on Location,” 2014 IEEE conference.

[13] Narayan Ranjan Chakraborty, Muhammad Taifur Rahman, Md. Ekhlasur Rahman, Mohammad Shorif Uddin, “Generation and Verification of Digital Signature with Two-factor Authentication”, 2016 International Workshop on Computational Intelligence (IWCI) 12-13 December 2016, Dhaka, Bangladesh .

[14] Niraj Kumar, Pankaj Gupta, Monika Sahu, Dr. M A Rizvi, “Boolean Algebra based Effective and Efficient Asymmetric Key Cryptography Algorithm: BAC Algorithm”, 2013 IEEE.

[15] Richard Bassous, Huirong Fu and Ye Zhu, “Ambiguous Asymmetric Schemes”, 2016 International Conference on Computational Science and Computational Intelligence.