INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE AND MANAGEMENT

CONTENTS

CALL FOR MANUSCRIPTS

We invite original research papers in the area of computer, finance, marketing, HRM, Banking, Insurance, and other allied subjects. The above mentioned tracks are only indicative, and not exhaustive. The journal expects unpublished and original quality research articles/papers only.

You may submit your articles/papers at the email addresses, info@ijrcm.org.in or infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. COVERING LETTER FOR SUBMISSION:

The Editor
IJRCM

Subject: **Submission of Manuscript**.

Dear Sir/Madam,

Find my submission of manuscript for possible publications in your e-journal.

I hereby affirm that the content of this manuscript are original. Furthermore it has been neither published elsewhere fully or partially or any language nor submitted for publication (fully or partially) elsewhere simultaneously.

I affirm that the all author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name(s) as co-author(s).

Also, if our manuscript is accepted, I/We agree to comply with the formalities as given on the website of journal & you are free to publish our contribution to any of your two journals i.e. International Journal of Research in Commerce & Management or International Journal of Research in Computer Application & Management..

Name of Corresponding Author (s)

Designation:

Affiliation:

Mailing address:

Mobile Number (s):

Landline Number (s):

E-mail Address (s):

2. **INTRODUCTION:** Manuscript must be in English prepared on a standard A4 size paper setting. It must be prepared on a double space and single column with 1" margin set for top, bottom, left and right. It should be typed in 12 point Calibri Font with page numbers at the bottom and centre of the every page.
3. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.
4. **AUTHOR NAME(S) & AFFILIATIONS:** The author (s) full name, designation, affiliation (s), address, mobile/landline numbers, and email/alternate email address should be in 12-point Calibri Font. It must be centered underneath the title.
5. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 300 words. The abstract must be informative and explain background, aims, methods, results and conclusion.
6. **KEYWORDS:** Abstract must be followed by list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stop at the end.
7. **HEADINGS:** All the headings and sub-headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
8. **MAIN TEXT:** The main text should be in a 8 point Calibri Font, single spaced, fully justified.
9. **FIGURES &TABLES:** These must be simple, centered & numbered, and table titles must be above the tables. Sources of data should be mentioned below the table.
10. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to Harvard Style of Referencing. The list of all references should be

alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow the references as per following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order…
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- Note that italics are used only for titles of books and names of journals. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- Use endnotes rather than footnotes.
- The location of endnotes within the text should be indicated by superscript numbers.
- For sources which have insufficient details to be included in the Reference, use endnotes (such as interviews, some media sources, some Internet sources).

SEE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

Books

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio," Ohio State University.

Contributions to books

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

Journal and other articles

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.
- Kiran Ravi, Kaur Manpreet (2008), Global Competitiveness and Total Factor Productivity in Indian Manufacturing, International Journal of Indian Culture and Business Management, Vol. 1, No.4 pp. 434-449.

Conference papers

- Chandel K.S. (2009): "Ethics in Commerce Education." Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

Unpublished dissertations and theses

- Kumar S. (2006): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University.

Online resources

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

Website

- Kelkar V. (2009): Towards a New Natural Gas Policy, Economic and Political Weekly, Viewed on 11 September 2009 http://epw.in/epw/user/viewabstract.jsp

A COGNIZANCE TO INFORMATION SECURITY

SHAILESH MAHESHWARI
ASST. PROFESSOR
SHRI VAISHNAV INSTITUTE OF MANAGEMENT
INDORE

ABSTRACT

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.[1]The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

In this paper, I show how our secured multiparty computation protocols protect the data of an organization during the war from the cyberspace war when a large number of defense units interact with one another, while hiding the identity and computations done by them. SMC is a problem of information security when large organizations interact with one another for huge data sharing and data exchange. It is quite possible that during sharing and exchange, the private data also get hacked. In order to protect and secure the private data, the protocols of SMC need to be deployed in the large computer networks on which the organizations work. The protocols work at the micro-level in terms of cryptography with which the data are encrypted and then shared, while allowing the keys to be used for sharable data while also keeping the keys untouched for private data. At the macro level, multilevel architectures are used for different types of security to be achieved. The computation part of the secured multiparty computation is based on the algorithmic complexity theory. The algorithms realize the protocols in such a way that it is tedious to break (decrypt) the keys to hack the private data.

KEYWORDS

Trusted third party (TTP), Secure multiparty computation (SMC), Cyberspace, Protocol

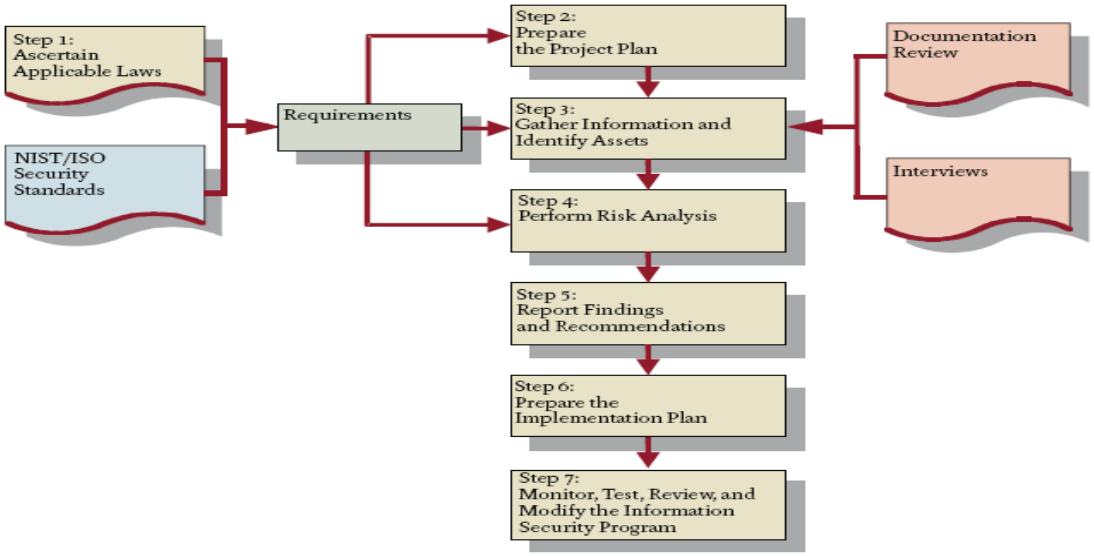
INTRODUCTION

With rapid technology and cost reduction, we have built a large Internet. The critical application of an organization requires an Internet to deliver information. The cyber world has become an important part of our day-to-day lives. Most of us use cyber space to communicate with friends and business associates through the devices that are connected to the Internet via wired or wireless technology. We make airline, railway and other travel reservations through the Internet, which we call the World Wide Web. Apart from this we use it for weather forecasting and planning of our daily activity, including our hobby and other social activities. We use the Web and all its powerful resources to educate ourselves and to gain knowledge. In summary, now cyber space is fully embedded in our daily live.

A common person connects to get information from home, office, university, or from any cyber cafe, even information stored in a remote place, so prevention is required. During war, millions of users wish to access the information which can be made accessible on the Internet. Many of the governmental decision-making processes also use cyber space to perform joint computations during war time. To prevent the identity of a defense unit, SMC can be applicable. When countries want to share the critical information of the war or terrorist attack, the terrorists can perform the malicious activities. They can capture the data from cyber space during communication, or a central computation body can disclose the information of one to others. This issue threatens all of us and introduces a whole set of ethical and legal issues for business people, scientists, parents, educators, and lawmakers.

In this paper, we propose and work out a technique to secure cyber space using SMC in which the data are concealed even from the anonymizers to further ensure privacy. The technique is based on encryption protocol working on multilayer SMC architecture. Solution involves the formal description of the protocol along with results to achieving high security. In this paper, we also address the issue of different adversaries in SMC and minimize their effects. In the SMC, a set of parties wishes to jointly compute some function of their inputs. Such a computation must preserve certain security properties, such as privacy and correctness; however, some of the participating parties or an external adversary colludes to attack the honest parties. While assuming that the result computed by a central body is trustworthy, we basically emphasize to hide the data of individuals. In proposed protocol, each party (country) will send encrypted data instead of original as well as the key to decrypt the same at a later stage of need. The party transfers key and data to TTP through a separate anonymizer for secrecy of key as well as data. In as earlier work, we had assumed that anonymizer will not store any data at any moment and shall only redirect it to the TTP. In addition to providing macro-level privacy, we also include micro-level in our proposed SMC protocol.

FIGURE 1. A TYPICAL INFORMATION SECURITY COMPLIANCE ASSESSMENT



LITERATURE REVIEW

With the increasing use of the Internet and deployment of various devices over the Internet, the risk of Security threats to privacy have become a major issue. Many sensors, monitoring devices, and environment data collecting devices are being deployed and have became an essential part of our daily life. Looking to such demanding needs, Cyber Trust Program at the National Science Foundation has increased the financial investment of research in this area. Business and individual organizations are facing cyber space security threats. The damage done by these threats is mounting along with the increase in the areas which are becoming their prey. The ability of resources, technology, and finances to cope with these is limited, however.

An individual, business, or enterprise system, that is, every critical system in cyber space, is a target of cyber threats. But there exist a possibility of forming a unified and effectual agenda for it by concentrating on severe threats that could cause critical damage.

Decision time, magnitude of threat, and awareness are the three key attributions of cyber space threat which are believed to have strong relations among them. Decision time refers to the pressure to the time approved for policy making; magnitude of threat means the matter's significance which is intimidating nations fundamental value; and the level of immediate grasp of the intermittent situation is the awareness (Michael, 2000).

Cyber space has become an important part of our daily life, consuming an escalating amount of our lives. It is increasingly being used for communication with friends, acquaintances, business associates, purchasing, selling goods and services, ticket reservations, weather Forecasts, news, social and travel planning, education, research, and as a source of information.

To protect the data of an individual from cyber space, SMC performs the major roles. SMC is the problem of *n* parties to compute a private function of their inputs in a secure method, where security means the correct result computed by a trusted third Party (TTP) for maintaining the privacy of the parties, as some of the parties may want to misuse another party's data. We assume that we have inputs *x1*, *x2*, . . ., *xn*, where *xi* is the data of party *Pi* and the TTP will compute a function *f* (*x1*, *x2*, . . ., *xn*) = (*y1*, *y2*, . . ., *yn*) and send the results to respective parties so that party *Pi* will receive only *yi* and not the results of other parties. This implies the data of all parties must be secure. Security is meant to achieve correctness of the result of computation and keep the party's input private, even when some of the parties are corrupted.

It is widely used to provide digital security of data as well as used in SMC protocol where malicious adversary exists. We had presented an SMC architecture in which the protocol tries to hide the identity of parties using some anonymizers. The *k* adversary parties hack the data of a party requires total permutations (*n*-*k*), which cannot be completed in polynomial time. This problem of insecure communication has been solved to some limit by introducing one more packet layers between anonymizer and party. This protocol is also used to secure Indian BPO. There is no attention given between anonymizer and TTPs that may cause the leakage of data through TTP. A Zero-Hacking protocol has been introduced which overcomes this problem using multiple TTPs. In this protocol, the computation is done by a randomly selected master TTP; thus the party is not aware where the computation will take place. So, it is difficult to disclose data through TTP. Also, the minimum number of TTP must be three. After this, to minimize risk we use encryption before sending the data to the anonymizer. To secure the data of an individual in cyber space, we propose a new protocol in which we divide and encrypt the data into packets of the parties before sending them to anonymizers.

DESIGN CONSIDERATIONS

PROTOCOL

Definition: 1. code of conduct or rules of appropriate behavior; 2. a formal agreement, in politics; 3. an original draft or record of a document
Synonyms: etiquette, rules, conventions, formalities, agreement
Antonyms:
Tips: Protocol is a diplomatic and political term that refers to appropriate behavior and rules of conduct for a particular situation or event. Protocol can also be a more sophisticated word to use to denote appropriate actions or rules in business (see usage examples). Protocol can also be used as a verb, meaning "to draw up or issue a protocol," but is most often used to refer to rules or conventions.

Usage Examples:
Business protocol requires that we arrive at this meeting well-prepared and on time. (etiquette)
We currently have several security protocols in place to insure that any sensitive company information is protected. (rules)
The countries established a new trade protocol to help further their respective economies and relations with each other. (agreement)
Carrie broke company protocol when she used her work e-mail address to send personal e-mails. (rules, conventions)
In network protocol, the data are encrypted and divided into a number of packets, and then the security increases the number of anonymizers that will behave as malicious adversaries. The main emphasis of this protocol is to minimize the effect of malicious adversaries. Figure 2 depicts that *p1*, *p2*. . . *on* are parties (countries). They encrypt the data through some predefined encryption technique. After encryption, encrypted data are divided into number of packets with corresponding packets holding encryption information. *D11*, *D12*. *Dij* are the different packets shown in Figure 2 where *I* = 1 . . . *n* and *j* = 1 . . . *d*. These packets go to randomly selected anonymizers *A1*, *A2*. *Am*. Anonymizer redirects these packets to TTP (computation body) for computation; here we are assuming that there is no loss of packets during the computation.

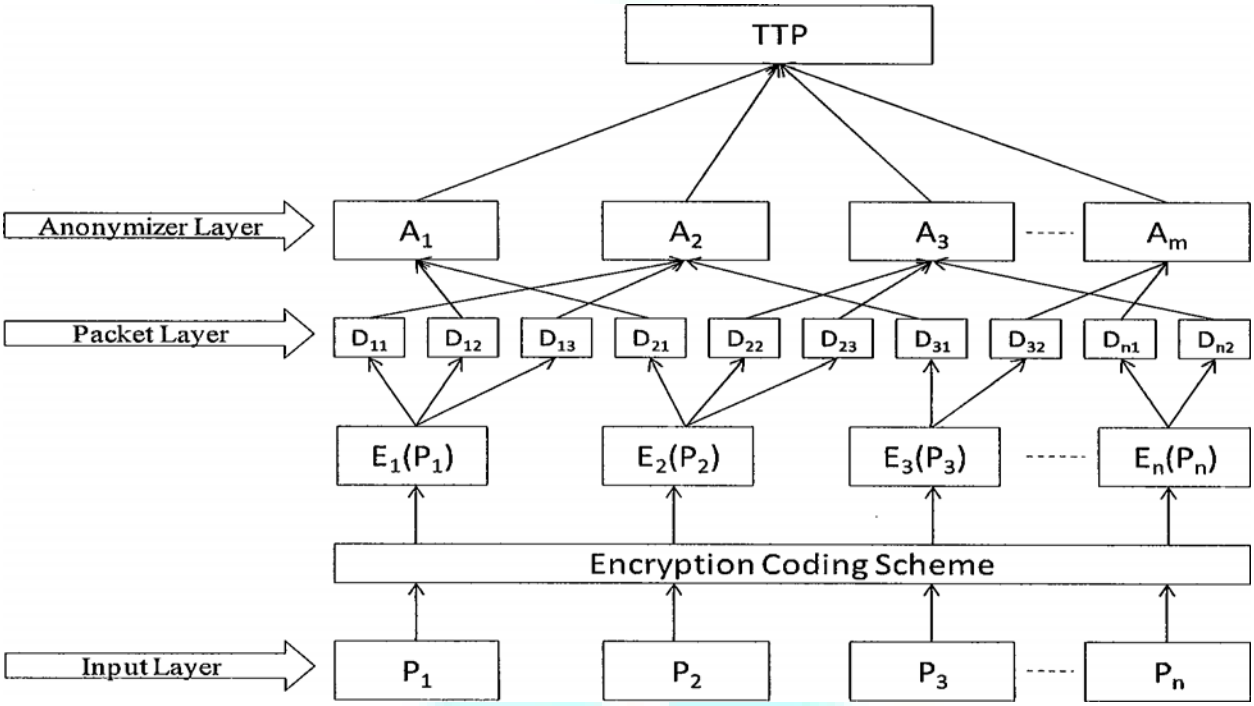


FIGURE 2 Architecture of protocol to protect cyber space.

CONCLUSION

The security of the system increases exponentially as the number of anonymizers increases. It is also concluded that even if the entire data of one party go through a single anonymizer, then security is also high. To further increase security, we divide the data in packets after encryption. The packets are then sent into different anonymizers. Because the packets are distributed among several anonymizers, one anonymizer cannot hold the entire data of any party. This paper also concludes that when data are encrypted and divided into a number of packets, then the security increases and even some of the anonymizers will behave as malicious adversaries. When we increase the number of packets, the security increases exponentially and the effect of the adversary minimizes. Therefore, the cyber space security is controlled using the encryption and anonymization process jointly.

REFERENCES

Jarvenpaa, S and Todd P, "Consumer's Reactions to Electronic Shopping on the World Wide Web",
Solange Ghernaouti Helie, Increase Trust and Confidence in Information and Communication Technology by a Multidisciplinary Approach.
Information Security Journal: A Global Perspective
C., Murat, K.,Jaideep, V., Lin, X.,and Michael, Y.(2002). Tools for privacy preserving distributed data mining.
Yao A.C. (1982). Protocols for secure computations. Proceeding of twenty third IEEE Symposium on the Foundation of Computer Science.
Fiallo, E.H. (2002). The lack of ethics in cyber space: A case for cyber ethics.
Dhillon, Gurpreet (2007). Principles of Information Systems Security: text and cases. NY: John Wiley & Sons.
The Complete Reference Network Security
Layton, Timothy P. (2007). Information Security: Design, Implementation, Measurement, and Compliance.
Bruce Schneier: Secrets & Lies: Digital Security in a Networked World, ISBN 0-471-25311-1
www.wisegeek.com/what-is-information-security.
egovstandards.gov.in/standards_network_app
en.wikipedia.org/wiki/Information_security

REQUEST FOR FEEDBACK

Esteemed & Most Respected Reader,

At the very outset, International Journal of Research in Commerce and Management (IJRCM) appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to take this opportunity to request to your good self to supply your critical comments & suggestions about the material published in this issue as well as on the journal as a whole, on our E-mails i.e. **info@ijrcm.org.in** or **infoijrcm@gmail.com** for further improvements in the interest of research.

If your good-self have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

Hoping an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator