Securing The Sensitive Information: Does It Really Happen?

Shalini Puri
M. Tech. Student
Birla Institute of Technology, Mesra
Ranchi, Jharkhand, India
eng.shalinipuri30@gmail.com

Sona Kaushik
M. Tech. Student
Birla Institute of Technology, Mesra
Ranchi, Jharkhand, India
sonakaushik22@gmail.com

Abstract— **Today, the security of sensitive information has become an essential and desired part of every organization, industry, enterprise, management system and even for the individual entity. It plays an important, challenging and vital role to provide high level protection against attacks using various techniques, methodologies and algorithms. These techniques are based on the primary concerns of security, i.e. data confidentiality, integrity, availability, and access control. With this, the provision of security is used to secure and protect highly sensitive data. In this paper, a technical review and a comparative study of different Sensitive Information Security (SIS) models, techniques and related concerns with their respective issues are discussed. This comparative study shows how different applications and key areas having very sensitive information are subjected to high security. Some of the models and surveys are based on the primary concerns of data security, whereas others provide the design of high or multi level security methods especially for specific systems. Therefore, such review and study provides a step to conclude that sensitive information of various applications around us must be provided the hard level security, so that such delicate and important information and data can be sent securely over on the unsecured communication channel. This paper provides a way ahead to rethink over on the Sensitive Information Security Provision.**

***Keywords-** sensitive information; data security; confidentiality; integrity; denial of service; usability; robustness*

I. Introduction

Highly Sensitive Information, Its Protection, and Secured Transmission against Enormous Attackers and Hackers! – It naturally tells us to get well prepared against them and play an edge to edge cut war. But this is not just as simple as it looks like. The complexity encapsulated in such security involves the highly complex security design which must be architecturally implemented by keeping an eye on all the primary and demanding issues of the security provision. As with the advancement of technology and fast access speed with high use of unsecured network, like Internet, the sensitive information and data essentially need to be provided high security either at the user end, at the receiver end or on the communication channel [1]. As the demand of the information transfer is increasing day- by – day, its security and protection mechanisms and methods are also increased. A lot of research work has been done and still going on Sensitive Information Security (SIS) models, related techniques and methodologies. In this direction, many different methods have been introduced and successfully used by different organizations according to their system needs.

Protection of sensitive information [1] - [10] is a growing concern around the world and typically, requires a great attention in various application fields and areas. For this, the security of critical information and data is demanded in all sectors, including the business, healthcare, banking, army and military, transportation systems, advertising industry, game playing and many more. Nowadays, this requirement has become the foremost priority of sensitive information management [1].

The primary and important concerns of data security, data confidentiality, integrity, access control and availability, are always desired desperately and wanted importantly. Usually, each concern needs a good level of attention when sensitive information security (SIS) models are developed. The necessity of quality issues related to the security, like robustness, usability etc, are equally important and required along with these security concerns. A lot of research work has been done and in process to have the best security technique. Although these models work on the sensitive information or data yet there is scope to extend such concepts to transfer very bulky and a large volume of sensitive data. Many applications consist of such information and require good protection mechanism.

Section II discusses the background of sensitive information security of different application key areas and sectors. Section III discusses a comparative study showing the different research methodologies of application key areas. Section IV discusses the conclusion of the paper.

II. Background

The development of sensitive and critical systems security over the last decades has boomed up a lot and made an important place in the research area. The critical information security issues and area of concerns are the red hot issues while important and sensitive information and data is sent over on the unsecured communication channel. The research work done shows the great results to provide the good security to the information and data with high level of techniques, mechanisms and methodologies.

The requirements of the information security systems which contain critical and sensitive data and information always essentially need high security. If such security cannot be held, then that system is open for the attackers and hackers. With such idea, Figure 1 show that how the different 4 application areas, banking, hospitals, transportation, and military systems require the security to their data. So, they transmit information using some cryptographic scheme. The unsecured network; i.e., Internet, is generally used for the purpose. The attacker wants to have access of this information before they are transmitted via the Internet, but cannot succeed. Therefore, during transmission, they try to break their locks or security. If their attempt is successful, they will obviously be able to access those sensitive data and information. Otherwise, this information is sent securely and safely to the other end. In this way, figure 1 shows the significance of the Security of Information Systems for application areas.

Many researchers have come forward with their significant algorithms and models and provided new kinds of protective environments. Most of them have been working for enterprises, industries, and corporate. Many application areas and related research have worked upon it. The banking system [7] for secure e-banking systems includes effective countermeasures against financial fraud, cybercrime and their related malicious attacks. Medical related security systems [3] [6] [8] have shown their contribution to provide good measures for confidentiality, integrity, authentication, and access control. Military based applications [9] used a complex architecture and design for securing the critical information to keep them safe.

While playing the online games, like chess [9], the sensitive information can be insecure. In this lieu, [9] proposed the survey and mechanisms to make it secure and to enhance the security by controlling the access. The country wise transportation system [2] requires a highly complex and dedicated secure system to tackle the security concerns. Including this, the advertising system [10] also makes use of the secured system. There is many more application key areas related to the security of sensitive information that always require high security even at the cost of time. Therefore, research study shows and contributes in providing the best security to the sensitive and critical information systems and maintains the key concerns as per the required levels.

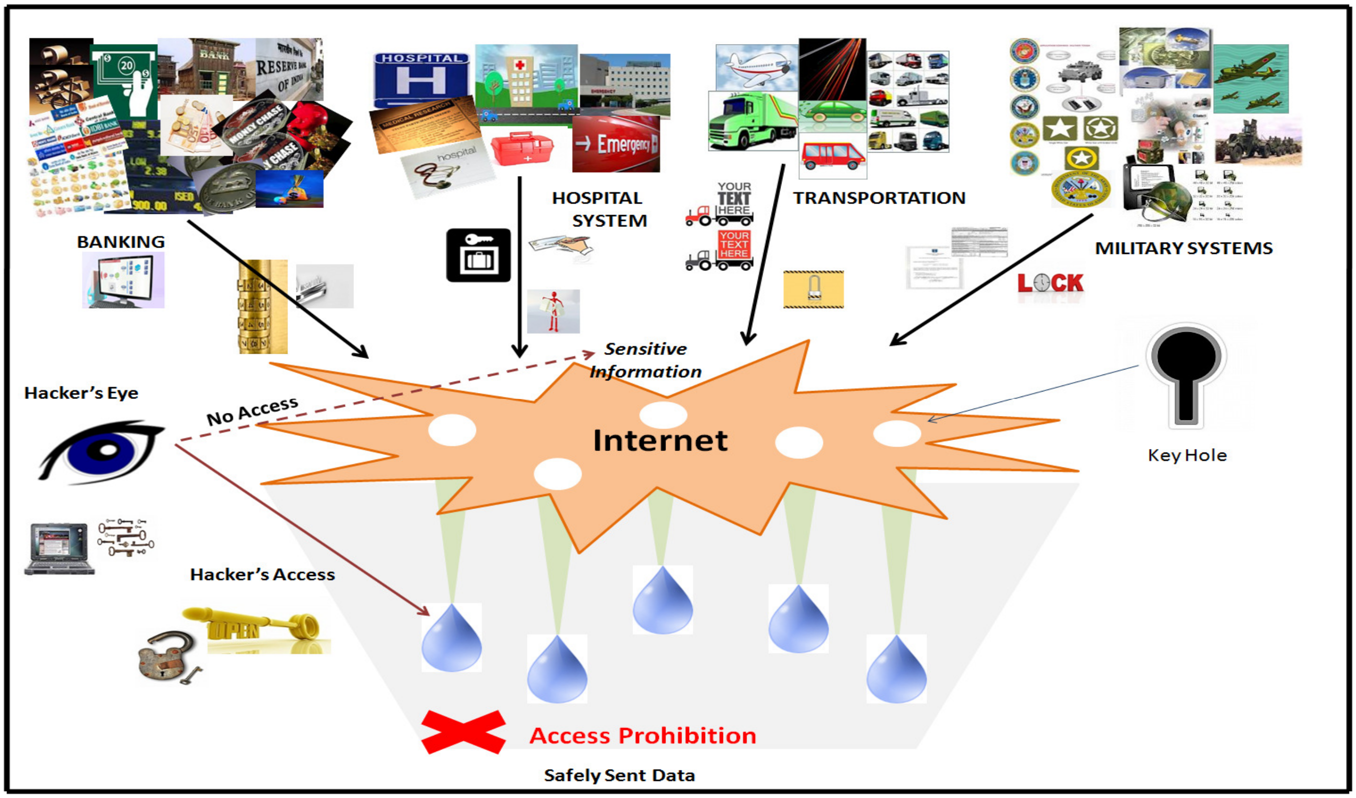

Figure 1. Attacks and Protection on the Sensitive Information Systems.

III. A Comparative Study of Various Application Key Areas

Based on the brief introduction given on the topic and substantiated by the background of the next section, a comparative study is given on the basis of technological advancements, methodologies and techniques proposed, for various application key areas. Table 1 shows the study to include the different application areas and fields in which sensitive information is sent usually and most of the times frequently. Such information needs to be provided best security with good quality key concerns. This study helps to show that many areas require to be kept secure from being theft and generate a protective environment to the world.

TABLE I. A COMPARATIVE STUDY OF VARIOUS APPLICATION KEY AREAS CONCERNED WITH SENSITIVE INFORMATION SECURITY

R N	Author(s) Problem Area	Solution Proposed	Primary Issue	Concepts Used	Experimental Results	Conclusion and Limitations
A. Health Care and Hospital Systems						
[3]	• Problem of moving an ICU patient's data from traditionally *isolated* hospital's computing facilities to data grids via public networks. • Need to establish integral and standardized security solution. • Need to put particular emphasis on the patient's personal data (Required by legislations in many countries of the European Union and world).	• A mandatory Access Control Model to protect patient's metadata. • A major security revision to previously proposed privacy protocol for "quality of security" quantitative metric to improve fragmented data's assurance.	• Patient' Consent: Authentication, Non-Repudiation, Integrity • Specific Purpose: Authorization, Confidentiality,Integrity • Privacy • Security	• Data Fragmentation • Health Grids • Intensive Care Grid (ICGrid) • Provides different levels of protection for metadata and data in order to mitigate vulnerabilities found with untrusted SEs and GC that could compromise sensitive material (i.e., patient's personal data). • Used a privacy protocol to protect the metadata and data, using a MAC for the former and cryptography with fragmentation for the latter.	• Configured a Grid Client, a Cent OS4-based ode as a "gLite user interface": An IBM xSeries 35 with two Intel Xeon HT processors @ 2.8 Hz and 2 GB of RAM. • DPM_mysql Storage Element (SE) running over Scientific Linux version 3.09. • A Dell PowerEdge1400, with two Intel Pentium III processors@800 MHz and 784 MB of RAM in SE. • One synthetic sample for 1 day of ICGrid's operation for a hospital (approximate 351 563 kB) for the data. • Use of gzip utility with its default parameters for compression at GC. • Use of aes-128-cbc algorithm1 from Open SSL library (version 0.9.8g) for SE encryption and decryption,. • Installation of a software-based bandwidth shaper at the GC. • Implementing Reed–Solomon IDA based on open-source code.	• Improves a patient personal data's security and privacy. • Achieves good performance. • Keep transferred data smallest as data transfer operations (upload and download) contribute with most of protocol's overhead. • Improvement in overall security greatly by using fragmentation as potential attackers, even with full control of one SE, compromises more SEs for 1 ICGrid file. • Used a test bed to measure expected performance with fragmentation and encryption methods.
[6]	Need to retain the privacy of the personal medical information using a simple and quick method of secure access to the medical data, without any delay the delivery of emergency care.	Presents architecture and a token based protocol for trust delegation on medical data across public mobile network & enables trust negotiation for highly secure environment to access confidential medical data.	• Response Time • Privacy • Trust	• Mobile Service Environment. • Trust Negotiation, Establishment and Termination in mobile devices. • Trust Negotiation between Mobile Emergency Medical Unit & Medical Record Database. • Downloading of Trust Delegated Medical Records onto the hand-held mobile devices of mobile emergency medical personal during emergency care. • Protect data from any unauthorized distribution and misuse. • Emergency Medical Units for sensitive personal medical records of unconscious patients.	.	• Introduced a scheme for trust lifecycle for mobile healthcare and secure storage of medical records for healthcare staff in public mobile communication networks. • Maintained the dynamic nature of the trust with the trust termination after the emergency medical care. • Forming a social business model with the contribution of security capsule scheme for healthcare industry to securely share medical data and services between service providers during emergency.
[8]	• Problem of Data Confidentiality for Healthcare and Medical Emergency System with accumulation of significant information. • Need of Multi - level security in emergency & E-user record & authentication for integrity.	• Provides information of confidentiality levels in database. • Provision of securing sensitive data Sensitivity at levels by Role-Base Security Policy.	• Data Confidentiality • Integrity	• Issue of information privacy using access control (user authentication and authorization) & Triple Encryption. • Application of cryptographic protocols for data transmission and storage. • Use of Web Server, Database, Telephony Server, SMS Server, Streaming Server for Medical Emergency System Architecture. • Use of Medical Emergency System Providers. Responder, EMT-Basic, EMT-Intermediate, Paramedic and Dispatcher	• Tested using WAPT (Web Application Performance Test) tool. • Performed Ramp up tests starting from 20 simultaneous clients to 200 clients to compute Response Time, Receiving Speed Per User, % of Errors.	• Comparing with normal system and existing security protocols such as SSL and, PGP. • Performed Encryption Decryption at low cost • Using the Double Layer Encryption in the proposed system to remove brute force attack weakness of SSL. • Confidentiality of some sensitive data.
B. Banking						
[7]	• Problem to check security and usability by existing evaluation methods Need of secure e-banking systems, and effective • Not addressing evaluation methods attempting to compare existing systems between conflicting demands of security and usability.	• A survey and study for interaction between security and usability of e-banking Security. • Proposed a theoretical evaluation framework to analyze the interaction and extrinsic factors. • Aligns security & usability for robust frame.	• Usability • Security	• Security Threat Model • Relevant Extrinsic Influence Factors: e-banking, security, usability, threat modeling, human-computer interaction for security.	• Quantitative Research: A representative survey of bank's public websites for information reviews on their primary e-banking security solutions on the top 10 banks (based on total assets) of all EU27 countries. • Qualitative Research: Threat Modelling of E-Banking Security Solutions, Content Analysis of E-Banking Usability Studies, Grounded Theory to Determine Extrinsic and, Modelling Relationship of Examined Factors, • Used a pattern to review all 27 EU countries, categories of e - banking security solutions: user name or ID / password combination, enhancement of 1. (e. g. memorable info), static OTP solutions (e. g. printed codes), dynamic OTP solutions (e. g. VASCO DigiPass), electronic signature / smartcard solutions, user system based solutions (e. g. certificates), & mobile authentication.	• Contributes in the practical value to banks, the potential for transfer to other business areas as well as the new insight and knowledge addition to the research area of usability for security. • Creating a more formal guideline for banks to ensure usable security of their e-banking systems. • Understanding and formalizing the relation and interplay between security and usability to improve e - banking systems for all users. • Provides countermeasures against financial fraud, cybercrime and their related malicious attacks.

C. Military Perspective						
[5]	Problem of IP over Satellite (IPoS) with intent to transit military communications to a network-centric (i.e. IP) mode of operation.	• A tactical military Ka-band Earth Terminal (ET) and waveform to support future mobile network-centric operation over conventional bent-pipe satellites. • Provision of reliable fill-mesh IP over satellite (IPoS) communications with uniqueness of mobile environment	• Security	• A waveform as the combination of baseband and RF signal structures, and protocols to implement communications over a SATCOM channel. • Two possible waveform reference models for support of IPoS: A Switch Model based on a selected terrestrial Link-layer standard, and A Router Model based on IP Network-layer protocols. • A prototype Ka-band Satellite Augmentation Terminal (KaSAT) for operation over the Wideband Gapfiller System (WGS). • Link layer switch and Network layer adaptation for KaSAT.	-	• An insignificant overhead by link-layer addressing. • Advantages of switch waveform model over router model at the SATCOM level: Simple, Stable, and network-layer independent waveform definition, based on Ethernet'802.3. • Use of an INE does not impact switch waveform protocols. • Disadvantages associated with the router based waveform model: Complex waveform definition and subject to potential change in network-layer protocols. • Blocking routing protocol exchange from/to an embedded ET gateway router and a remote edge router connected to node using INE.
D. Game Playing						
[9]	• Problem of not sufficiently providing sensitive information security by Internet Chess Club (ICC) to assure its users about security protocol used. • Flaws of ICC network security protocol and enabling passive eavesdroppers to listen in on communications and enabling active adversaries to mount severe attacks on ICC users.	• Shows the flaws how a passive adversary can easily read all communications with a trivial amount of computation, and how an active adversary can gain virtually unlimited powers over an ICC user. • Provide simple methods to defeat the timestamping mechanism.	• Security • Access Control • Assurance	• Cryptanalysis Lessons • Key Management • Reverse Engineering	-	• Timestamping mechanism to easily circumvent, allowing malicious users to cheat at chess by unfairly gaining time on the clock. • Very hard to devise security protocols.
E. Transportation System						
[2]	• Need an indicator of economic growth in countries. • Necessity to deploy an Intelligent Transportation System (ITS) in a cost effective and economic manner.	Design of an Intelligent Transportation System using Automated License Plate Recognition with Digital Image Processing.	Robustness	• Digital Image Processing • Automated License Plate Recognition (ALPR). • Automated License Segment Recognition (ALSR), IP Based ALPR Camera. • ITS with multiple layers (5 layers: base, layer I to III and top) of integrated innovative technologies: *Physical Layer* with deployment of high-speed secure information highway established with a national level computer backbone network, *Technological Layer* with IP based sophisticated intelligent Camera technologies and the application of intelligent algorithms on advanced digital image processing techniques, *Application Layer* with advanced application programs and databases implemented in the Open-Source Technology Stream deployed in Open Source Operating Systems. • Standardized Vehicle License Plate of ITS.	Layer wise implementation	• An imitative for common platform with DIP for ITS component modules. • Intelligent algorithms on advanced DIP techniques in a multi-layer architecture and deployed in multiple stages to make the system robust and making the environment gradually standardized, without much disturbances. • Further reduction of development and deployment cost with Open Source Operating System. • Disadvantages with DIP in designing component modules of ITS: Heterogeneous Environment, Heterogeneous Traffic Conditions, Quality Variation of Captured Image/Video, Offline & Real Time Image Processing. • Lack of DIP techniques on streaming video.
F. Advertising Industry						
[10]	Problem of curse of high dimensionality in high-dimensional, and resulting in useless data for further data analysis privacy problem in a real-life mashup	A service-oriented architecture along with privacy - preserving data mashup algorithm.	Preserve privacy and information utility on the mash up data. Privacy Protection	• Anonymity • Data mashup • Data Integration • Service-oriented architecture • Join multiple private data sets together to reveal the sensitive information to the other data providers. • Sharpen the identification of individuals using integrated (mashup) data to reveal their person-specific sensitive information (not available	• Mashup in distributed web service environment, running each data provider on an Intel Core2 Quad Q6600 2.4GHz PC with 2GB RAM connected to a LAN. • Collected Adult data set of 6 numerical attributes, 8 categorical attributes, & a binary Class attribute. • Using 2 income levels ≥ 50K. • Considered Divorced and Separated in attribute Marital-status as sensitive, and the remaining 13 attributes as QID.	• To achieve the LKC-privacy on the mashup data without revealing more detailed information in process. • Compared to classic secure multiparty computation, allows data sharing instead of only result sharing. • Demands anonymization methods to preserve information for various data

	application.			before the mashup). • Many data attributes in the mashup data from multiple sources.	• Evaluate impacts on classification quality, collected several classification errors & MCE from testing set: Baseline Error (BE) is error measured on 14 raw data attributes. • Evaluate impact of dimensionality: number of QID attributes on data quality for distortion metric using at most 20 secs for previous experiments. • Combining training and testing sets, giving 45,222 records, and for each original record.	analysis tasks. • A simple privacy model. • Intuitive to understand and to explain to the clients.
G. Extraneous						
[1]	• Inadequacy and insufficiency of security measures of existing techniques. • Attacks on user interface through open networks.	A Security architecture (SecureSIS) with four "tangible" components:	• Confidential channel • Authentication for user interface • Data encryption at storage	• Formal definition and cryptographic properties proofs of dynamic keys. • Feature of intrusion prevention and detection using 2 sets of dynamic keys. • Dynamic Key management (DKM). • User-Oriented Group Key Management (UGKM), Authentication and Authorization Management (AAM), Sensitive Information management (SIM), & 2 "intangible" components: Security Agreement (SA) & Security Goals.	-	• New proposed security architecture. • To develop knowledge surrounding sensitive information protection. • Overcomes limitations of existing security approaches in protecting sensitive information.
[4]	Problem of Evil Twin attacks of rogue wireless access point to intercept traffic between mobile users and Internet.	Providing "end-to-middle security," to be adopted by mobile users.	End to middle security	• Uses a virtual gateway to relay traffic for mobile users. • Target on the less programmable mobile devices such as game consoles and VoIP phones.	• VPN, Web Proxy, and Voice Gateway to implement end to middle security. • User-centric.	An end-to-middle security model, adopted by mobile users to protect themselves against Evil Twin attacks.

IV. Conclusion

The security of highly sensitive information and data is essential and required inside and outside of the system. Such data security and protection must be ensured at its best level concerning its primary issues. Many new models with good techniques and methods have been introduced and successfully used. The comparative study puts an effort to check their key areas and solutions for the given problems. This research has presented a security overview and study that show the applications based security algorithms and approaches in protecting sensitive information. These approaches demonstrate the protection of the critical information of various applications from the attacks, hacking, and intrusions. Such study shows that there is always a need of these systems and such new models to keep all the attackers and hackers silent. This mechanism has yet to be studied formally and systematically. It could be further investigated. This direction for security is provided in the form of the security provision for application key areas. It could help in order to enhance the security of other sensitive information systems.

Acknowledgment

We would like to acknowledge and give our special thanks to Asst. Prof. Pankaj Gupta, Dept. of Computer Science, Birla Institute of Technology, Noida, India and Dr. Vikas Saxena, Dept. of Computer Science, Jaypee Institute of Information Technology, Noida, India for their continuous encouragement, help and guidance.

References

[1] X. Wu, P. D. Le, and B. Srinivasan, "Security Architeture for Sensitive Information Systems," Convergence and Hybrid Information Technologies, pp. 239 – 266, March 2010.

[2] M. Padmadas, K. Nallaperumal, V. Mualidharan, and P. Ravikumar, "A Deployable Architecture of Intelligent Transportation System - A Developing Country Perspective," IEEE International Conference on Computational Intelligence and Computing Research, pp. 1 - 6, 2010.

[3] J. Luna, M. Dikaiakos, M. Marazakis, and T. Kyprianou, "Data-Centric Privacy Protocol for Intensive Care Grids," IEEE Transactions on Information Technology in Biomedicine, vol. 14, issue 6, pp.1327 - 1337, 2010.

[4] E. Y. Chen, and M. Ito, "Using End-to-Middle Security to Protect against Evil Twin Access Points," IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops, pp. 1 - 6, 2009.

[5] M. A. Cusano, and M. Sullivan, "Layered Architecture Considerations in the Development Mobile Tactical Environment of a Network-Cent SATCOM Waveform Definition for the Mobile Tactical Environment," Military Communications Conference, IEEE, vol. 2, pp. 679 - 682, 2004.

[6] D. Weerasinghe, and R. Muttukrishnan, "Secure Trust Delegation for Sharing Patient Medical Records in a Mobile Environment," IEEE 7th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1 - 4, 2011.

[7] C. Mockel, "Usability and Security in EU E-Banking Systems," IEEE/IPSJ 11th International Symposium on Applications and the Internet, pp. 230 – 233, 2011.

[8] S. A. Hameed, H. Yuchoh, and W. F. Al-khateeb, "A Model for Ensuring Data Confidentiality in Healthcare and Medical Emergency," IEEE 4th International Conference on Mechatronics, pp. 1 - 5, 2011.

[9] J. Black, M. Cochran, and R. Gardner, "Lessons Learned: A Security Analysis of the Internet Chess Club Black," 21st Annual Computer Security Applications Conference, IEEE, pp. 245 – 253, 2005.

[10] B. Fung, T. Trojer, P. Hung, L. Xiong,, K. Al-Hussaeni, and R. Dssouli, "Service-Oriented Architecture for High-Dimensional Private Data Mashup," IEEE Transactions on Services Computing, 2011. (Unpublished).