**Chapter 2**

**Review of related literature**

The researchers found the following studies and literature that are relevant to the system proposed.

**Lumad**

Lumad, the self-ascription and collective identity of the 18 ethno-linguistic tribes in Mindanao. The Lumads have been long deprived of basic social services, particularly health and education. 9 out of 10 lumad children have no access to education and about 162 IP learning centers build all over Mindanao by NGOs & Church institutions are serving 6,000 Lumad children who are eager to learn.

**Basic Human Rights**

According to the Universal Declaration of Human Rights, created by the United Nations in 1948 to provide a global understanding of how to treat individuals, we have 30 basic human rights. Human rights allow a person to live with dignity and in peace, away from abuses the can be inflicted by abusive institutions or individuals. But the fact remains that there are rampant human rights violations around the world. Human rights is a global term we hear often, but many people can’t define. “Rights” are the things we are allowed to be, to do or have, simply by being human.

(Melody, 2009)

**Children’s Rights**

Children’s rights law is defined as the point where the law intersects with a child's life. That includes juvenile delinquency, due process for children involved in the criminal justice system, appropriate representation, and effective rehabilitative services; care and protection for children in state care; ensuring education for all children regardless of their race, gender, sexual-orientation, gender-identity, nationality and origin, religion, disability, [color](https://en.wikipedia.org/wiki/Human_skin_color), ethnicity, or other characteristics, and; health care and advocacy.

Children's rights are the human rights of children with particular attention to the rights of special protection and care afforded to minors. The Convention on the Rights of the Child (CRC) of 1989 defines a child as any human person who has not reached the age of eighteen years.

**Children’s Right to Education**

**Education is an essential right, which permits each person to receive instruction and to blossom socially. The right to an education is vital for the economic, social and cultural development of all societies.**

Education entails that its subjects acquire a variety of knowledge. It begins with the acquisition of elementary knowledge—that is to say, literacy—on the part of the youngest members of society. At this stage, children learn to read and write thanks to primary instruction and parental oversight. This is an essential stage which will permit the child to pursue his/her education by integrating secondary and post-secondary instruction.

Education also consists of a form of learning that is necessary for the development of one’s personality and identity, as well as his physical and intellectual capabilities. Education permits, notably, the transmission of common principles to new generations, and the conservation and perpetuation of social values. It also contributes to the flourishing of individuality through the enhancement of social and professional integration.

Education has as its ultimate objective the improvement of a person’s quality of life. It offers to underprivileged adults and children a chance to escape from poverty. It is thus an essential tool for the economic, social and cultural development of all populations around the world.

Education is a human right which ought to be accessible to everyone, without any discrimination. All children must be able to go to school, and thereby benefit from the same opportunities to build a future. Additionally, educational instruction must be equally gratuitous so that children from disadvantaged environments will be able to enjoy their right to an education. (Unicef, State of the World’s children 2010)

**Children’s Right in the Philippines**

Although the Philippines signed the Convention on the Rights of the Child in 1990, as of 2014, it is poorly enforced. Between 26 and 30 percent of the Filipino population lives below the poverty line, which causes hunger and malnutrition in children, and 22 percent of children are underweight, causing developmental disorders and diseases. Remote regions of the Philippines, where health care is almost nonexistent, are in dire need of medical aid. Academic, hygienic and medical health education is not widespread; only 67 of every 100 kids who begin elementary school ever graduate.

Ten to 12 percent of Filipino children are forced into child labor by parents to provide additional financial support. Most of these children work as scavengers in garbage dumps or as farmhands. The sex industry in the Philippines features heinous exploitation of children through sex trafficking, sex tourism and prostitution. These abuses are widespread and acknowledged but still commonplace. Children are often recruited by non-state groups and used as soldiers, especially by the New People's Army. The government has repeatedly killed or imprisoned children used by these groups. (Fau, 2011)

**Children’s Rights in Davao City**

Davao City heavily invests in various programs, policies, and services that promote and protect child rights. It allocated more than 300 million pesos for child-focused initiatives in 2014 alone; it also requires barangays to include in their respective annual budgets an allocation for Early Childhood Care and Development (ECCD) and the Barangay Council for the Protection of Children (BCPC). Among the LGU's achievements are the enactment of the Comprehensive Children and Family Support System in Davao City, otherwise known as the “Davao City Children’s Welfare Code”, as early as 1994, and the formation of the Davao City Council for the Welfare of Children (DCCWC) with a committee devoted to each of the four core rights of a child (survival, development, protection and participation). (UNICEF, 2016)

**About SOS network**

Under the Aquino administration children’s rights violations are rife, with military occupation of schools becoming out of control and interrupting the education of future generations. This must not be tolerated!

International laws covering conflict situations expressly prohibit the use of public infrastructures such as schools; hospitals and rural health units for military purposes such as command posts, barracks detachments, and supply depots.

Education is a basic human right, however over recent years there has been an alarming increase in the number of reports of schools being militarized, being used as barracks and detachments in the course of the Aquino government counter insurgency campaign.

This recurring child rights violations gave birth to the Save Our Schools network. **The Save our schools Network is a network of child rights advocates, organizations and various stakeholders working together to bring light and take action on the ongoing violation of children’s right to education, particularly those in the context of militarization and attacks on schools. (Wordpress, 2016)**

**Attacks on schools in Mindanao**

The last year of the Benigno S. Aquino presidency has meant a bloodbath for indigenous peoples and for Lumad education, two months after his State of the Nation Address where he gloated of figures that have purportedly addressed classroom shortages and increased the quality of Philippine education.

Emerito ‘Tatay Emok’ Samarca, executive director of the Alternative Learning Center for Agriculture and Development, Inc. (ALCADEV) and a convenor of the Save Our Schools Network was killed by government-backed indigenous paramilitary forces. His body was found lying in a pool of blood, with stab wounds on his neck, and his throat slit. While Dionel Campos, chairperson of MAPASU (Persevering Struggle for Future Manobo Generations), and his cousin Aurelio “Bello” Sinzo, were strafed dead before the terrified community of Han-ayan, Lianga town, Surigao del Sur province.

The paramilitary group Magahat/Bagani--- armed, controlled, and commanded by the 36th Infantry Battalion, Philippine Army---  burned down the school cooperative building and threatened to massacre the entire community if they would not leave the area two days before the killing of the Samarca, Campos, and Sinzo in the morning of September 1, 2015.

The dastardly crime which was perpetrated at dawn and later carried out in broad daylight, terrified the erstwhile peaceful Manobo school and community. As of this writing, the number of evacuees in Caraga has swelled to 3,000 individuals or more than 500 families coming from the municipalities of San Miguel and Lianga, with some 70 families still lost in nearby forests.

The Philippine military’s attack on ALCADEV using indigenous paramilitaries is by far the gravest and most vicious violation of indigenous peoples’ right to education and constitutes a wholesale violation of children’s rights.

Moreover, as schools are an integral part of communities, the attack is an open declaration of the Philippine state’s war of annihilation against people’s organizations and communities resisting foreign large-scale plunder of ancestral domains.

The 36th IB Philippine Army-Magahat/Bagani rampage at the ALCADEV School shows that the Aquino government has dropped all pretenses of adhering to the United Nations Convention on the Rights of the Child and other international human rights instruments. It also demonstrates the irrefutable crimes of the Philippine Army against indigenous children which the UN Special Representative of the Secretary General on Children and the Armed Conflict has continually glossed over, understated, or consistently concealed in its annual reports.

The Philippine government’s attacks on the ALCADEV School clearly shows its contempt towards self-determined development asserted by indigenous communities. Alternative Lumad schools are pushing for their own culturally-relevant pedagogy that liberates indigenous peoples from the yoke of institutionalized discrimination and corporate plunder of ancestral lands.

The Aquino government should be held accountable for all these violations. It is responsible for the formation and arming of the paramilitary groups, the paving the way for the entry of  large-scale destructive projects in the ancestral domains, the sowing of disunity among IPs, and the killings that have claimed the lives of many.

The Save Our Schools Network demands Justice for Samarca, Campos, Sinzo and all victims of human rights abuses! End all forms of attacks on schools and communities. (Templa, 2015)

**Military attacks on schools unabated – SOS Network**

The indigenous children’s right to education continues to be violated, as government seems to be hindering the operations of alternative schools, instead of recognizing their efforts, said the Save Our Schools Network.

MANILA – School administrators of the besieged Lumad schools in Mindanao are back in Manila to appeal to government agencies to stop the continuing military attacks in their schools, which, they said, violates the right to education of children of indigenous peoples (IP).

Although classes have resumed in the schools of the Salugpungan Ta’ Tanu Igkanugon Community Learning Center (STTICLC) and the Mindanao Interfaith Services Foundation Inc. (Misfi) Academy, soldiers and paramilitary men continue to harass students and teachers, the Save Our Schools Network said in a press conference on Monday, July 6.

Ronnie Garcia, Basic Education Principal of STTICLC, said soldiers continue to roam the area, branding teachers and the schools as “New Peoples’ Army (NPA) schools.” Soldiers have threatened families who enrolled their children in the Lumad schools that they will be disqualified from the Pantawid Pamilyang Pilipino Program. Worse, Garcia said, IP leaders have reported that soldiers told them to kill the teachers of the school. Benjamin Valbuena, national chairperson of the Alliance of Concerned Teachers, a member of the SOS Network, lamented that soldiers involved violated civilian authority, provoking people to murder instead of being the protector of the people and the state **(UMIL, 2015).**

**Network administration security and maintenance**

A **network administrator** maintains computer infrastructures with emphasis on networking. Responsibilities may vary between organizations, but on-site servers, software-network interactions as well as network integrity/resilience are the key areas of focus.

**Duties**

The role of the network administrator can vary significantly depending on an organization's size, location, and socio-economic considerations. Some organizations work on a user-to-technical support ratio, whilst others implement many other strategies.

Generally, in terms of reactive situations (i.e.: unexpected disruptions to service, or service improvements), IT Support Incidents are raised through an Issue tracking system. Typically, issues work their way through a Help desk and then flow through to the relevant technology area for resolution. In the case of a network related issue, an issue will be directed towards a network administrator. If a network administrator is unable to resolve an issue, a ticket will be escalated to a more senior network engineer for a restoration of service or a more appropriate skill group.

Network administrators are often involved in proactive work. This type of work will often include:

* Network monitoring
* Testing the network for weakness
* Keeping an eye out for needed updates
* Installing and implementing security programs
* In many cases, E-mail and Internet filters
* Evaluating implementing network

Network administrators are for making sure that computer hardware and network infrastructure related to an organization's data network are effectively maintained. In smaller organizations, they are typically involved in the procurement of new hardware, the rollout of new software, maintaining disk images for new computer installs, making sure that licenses are paid for and up to date for software that needs it, maintaining the standards for server installations and applications, monitoring the performance of the network, checking for security breaches, and poor data management practices. A common question for the small-medium business (SMB) network administrator is, how much bandwidth do I need to run my business? Typically, within a larger organization, these roles are split into multiple roles or functions across various divisions and are not actioned by the one individual. In other organizations, some of these roles mentioned are carried out by system administrators.

As with many technical roles, network administrator positions require a breadth of technical knowledge and the ability to learn the intricacies of new networking and server software packages quickly. Within smaller organizations, the more senior role of network engineer is sometimes attached to the responsibilities of the network administrator. It is common for smaller organizations to outsource this function. (Wikipedia, 2016).

# Security on the Internet, Then and Now

Back in the days before the Internet, “security” meant entering a password on your computer when you turned it on. Ah, what innocent times!

Computer viruses became an issue only when people began sharing files and using modems. In 1981 “Elk Clone” became the first widespread computer virus, reputedly spread from Texas A&M University. The term “computer virus” didn’t enter our lexicon until 1984, when introduced by an anti-virus software developer named Fred Cohen.

In our innocence, we protected ourselves by not using floppy disks without first scanning them for viruses. After all, viruses could only enter our system on infected floppies, right? Well, Ward Christensen and Randy Suess had already introduced the first computerized bulletin board system (BBS) in 1978, and with it the era of file sharing was begun. Eventually, bulletin boards became ubiquitous (I even ran one for a couple of years), and viruses had another way to infect our computers.

The Morris worm, a self-replicating UNIX-based program, was released by Cornell graduate student Robert Morris Jr. and brought about 10 percent of the computers on ARPANET (the precursor to the Internet) to their knees in 1988.

New threats materialized as hackers began using war dialers, computer programs that would dial every number in an interchange sequentially to determine if a modem was at the other end. Run it overnight and next morning the hacker had a list of modem phone numbers—which he or she could use to try to hack into the attached computer.

Literally and suddenly, the Internet changed everything. In 1993 the CERN research center in Geneva, Switzerland, introduced the first web browser, MOSAIC. The Internet now had a graphical interface just like Microsoft Windows. It was not just for geeks anymore. In June 1993 there were 130 websites worldwide. Today, it is estimated that there are more than 60 million.

Soon computer viruses were spreading through the Internet. Vulnerabilities in the Windows operating system (then and today) became apparent. Denial of service attacks brought down major Internet operations by using computers to log thousands of “users” into a website at the same time—all done automatically, sometimes through computers hijacked with a virus or worm. Antivirus programs became ubiquitous, and we all began to use words like “firewall” and “IP address” as though we understood the underlying concepts. In 1992 the number of computer-reported hacking incidents, viruses, and worm infections was relatively tiny. By 2002 it was in the hundreds of millions. New computer viruses had become front-page news.

In 1993 a Russian hacker group committed bank robbery over a network. In 1994 federal authorities captured Kevin Mitnick, the era’s most notorious computer hacker. He was charged with obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet service providers, and educational institutions, and stealing, copying, and misappropriating proprietary computer software. Mitnick was also in possession of 20,000 credit card numbers at the time of his arrest.

To our everlasting shame as lawyers, in 1994 one of the first “spam” messages was posted to newsgroups by two attorneys, Laurence Canter and Martha Siegel, offering their services in an upcoming U.S. “green card” lottery. A new industry (and annoyance) was born.

In 1997 Ian Goldberg, a University of California-Berkeley graduate student, took up a challenge by RSA Data Security, Inc., to crack its 40-bit encryption algorithm, then considered unbreakable. He did it in three and one-half hours. The message encrypted by RSA was, “This is why you should use a longer key.” Goldberg then successfully took up a challenge to break a 56-bit DES encryption algorithm (then the government standard). Today, folks routinely use 128-bit keys. And worry.

Soon we discovered that it wasn’t only computer programs (so-called executable files) that could contain viruses. The macro language in word processors such as Microsoft Word and WordPerfect were found to be vulnerable. One could merely open a document file and a malicious macro would wreak havoc. Vulnerabilities appeared not only in operating systems but also web browsers. Hackers could hide a program on your computer to do all kinds of nefarious things, including watching what you were doing; if your activities were of interest (e.g., entering a credit card number, a password, or the like), the program would report back to the hacker unbeknownst to you.

It got worse. Advertisers discovered the value of desktop space on your computer and found ways to put banner ads on your browser. Then they added so-called pop-ups that would mysteriously appear as a window on your computer monitor, often advertising the most embarrassing of services. To make matters worse, advertisers discovered that if they offered free software that did something useful, they could include “spyware” to track your shopping habits and report back to the vendor—who now had your name and e-mail address for a spam mailing list tailored to your interests. Less honest persons could do truly bad things with spyware, and the identity theft industry was born. Thus, too, was born a new software industry to prevent, discover, and remove adware and spyware.

With the Internet so intertwined with our law practices, computer security is not just a recommendation for attorneys; it’s an ethical requirement. Most of us now connect to the web via a high-speed cable or DSL hookup—always on, always available, and always potentially vulnerable. Antivirus software is essential, and it must be updated frequently. Firewalls, which limit the availability of connections to a computer on the Internet, are also a must.

# Today, security on the Internet is certainly not taken for granted. It requires diligence and attention, as well as a certain amount of technical capability. The threats are there—and as ingenious as only a worldwide community of miscreants could create.(Colidge, 2005).

# Database Security: What Students Need to Know

# Database security is a growing concern evidenced by an increase in the number of reported incidents of loss of or unauthorized exposure to sensitive data. As the amount of data collected, retained and shared electronically expands, so does the need to understand database security. The Defense Information Systems Agency of the US Department of Defense (2004), in its Database Security Technical Implementation Guide, states that database security should provide controlled, protected access to the contents of a database as well as preserve the integrity, consistency, and overall quality of the data. Students in the computing disciplines must develop an understanding of the issues and challenges related to database security and must be able to identify possible solutions. At its core, database security strives to insure that only authenticated users perform authorized activities at authorized times. While database security incorporates a wide array of security topics, notwithstanding, physical security, network security, encryption and authentication, this paper focuses on the concepts and mechanisms particular to securing data. Within that context, database security encompasses three constructs: confidentiality or protection of data from unauthorized disclosure, integrity or prevention from unauthorized data access, and availability or the identification of and recovery from hardware and software errors or malicious activity resulting in the denial of data availability.

# In the computing discipline curricula, database security is often included as a topic in an introductory database or introductory computer security course. This paper presents a set of sub-topics that might be included in a database security component of such a course. Mapping to the three constructs of data security, these topics include access control, application access, vulnerability, inference, and auditing mechanisms. Access control is the process by which rights and privileges are assigned to users and database objects. Application access addresses the need to assign appropriate access rights to external applications requiring a database connection. Vulnerability refers to weaknesses that allow malicious users to exploit resources. Inference refers to the use of legitimate data to infer unknown information without having rights to directly retrieve that information. Database auditing tracks database access and user activity providing a way to identify breaches that have occurred so that corrective action might be taken.

Database technologies are a core component of many computing systems. They allow data to be retained and shared electronically and the amount of data contained in these systems continues to grow at an exponential rate. So does the need to insure the integrity of the data and secure the data from unintended access. The Privacy Rights Clearing House (2010) reports that more than 345 million customer records have been lost or stolen since 2005 when they began tracking data breach incidents, and the Ponemon Institute reports the average cost of a data breach has risen to $202 per customer record (Ponemon, 2009). In August 2009, criminal indictments were handed down in the United States to three perpetrators accused of carrying out the single largest data security breach recorded to date. These hackers allegedly stole over 130 million credit and debit card numbers by exploiting a well known database vulnerability, a SQL injection (Phifer, 2010). The Verizon Business Risk Team, who have been reporting data breach statistics since 2004, examined 90 breaches during the 2008 calendar year. They reported that more than 285 million records had been compromised, a number exceeding the combined total from all prior years of study (Baker et al., 2009). Their findings provide insight into who commits these acts and how they occur. Consistently, they have found that most data breaches originate from external sources, with 75% of the incidents coming from outside the organization as compared to 20% coming from inside. They also report that 91% of the compromised records were linked to organized criminal groups. Further, they cite that the majority of breaches result from hacking and malware often facilitated by errors committed by the victim, i.e., the database owner.

Unauthorized access and SQL injection were found to be the two most common forms of hacking, an interesting finding given that both of these exploits are well known and often preventable. Given the increasing number of beaches to database systems, there is a corresponding need to increase awareness of how to properly protect and monitor database systems. At its core, database security strives to insure that only authenticated users perform authorized activities at authorized times. It includes the system, processes, and procedures that protect a database from unintended activity. The Defense Information Systems Agency of the US Department of Defense (2004), in its Database Security Technical Implementation Guide, states that database security should provide “controlled, protected access to the contents of your database and, in the process, preserve the integrity, consistency, and overall quality of your data” (p. 9). The goal is simple, the path to achieving the goal, a bit more complex. Traditionally database security focused on user authentication and managing user privileges to database objects (Guimaraes, 2006).

This has proven to be inadequate given the growing number of successful database hacking incidents and the increase in the number of organizations reporting loss of sensitive data. A more comprehensive view of database security is needed, and it is becoming imperative for students in the computing disciplines to develop an understanding of the issues and challenges related to database security and to identify possible solutions. Database security is often included as a topic in an introductory database course or introductory computer security course. However as the knowledge base related to database security continues to grow, so do the challenges of effectively conveying the material. Further, many topics related to database security are complex and require students to engage in active learning to fully com- Murray IIP-63 prehend the fundamental nature of database security issues. This paper presents a set of subtopics for inclusion in a database security component of a course. These sub-topics are illustrated using a set of interactive software modules.

**Access Control**

The primary method used to protect data is limiting access to the data. This can be done through authentication, authorization, and access control. These three mechanisms are distinctly different but usually used in combination with a focus on access control for granularity in assigning rights to specific objects and users. For instance, most database systems use some form of authentication, such as username and password, to restrict access to the system. Further, most users are authorized or assigned defined privileges to specific resources. Access control further refines the process by assigning rights and privileges to specific data objects and data sets. Within a database, these objects usually include tables, views, rows, and columns. For instance, StudentA may be given login rights to the University database with authorization privileges of a student user which include read-only privileges for the Course\_ Listing data table. Through this granular level of access control, students may be given the ability to browse course offerings but not to peruse grades assigned to their classmates. Many students, today, inherently understand the need for granularity in granting access when framed in terms of granting ‘friends’ access to their Facebook site.

**Database Vulnerability**

Security breaches are an increasing phenomenon. As more and more databases are made accessible via the Internet and web-based applications, their exposure to security threats will rise. The objective is to reduce susceptibility to these threats. Perhaps the most publicized database application vulnerability has been the SQL injection. SQL injections provide excellent examples for discussing security as they embody one of the most important database security issues, risks inherent to non-validated user input. SQL injections can happen when SQL statements are dynamically created using user input. The threat occurs when users enter malicious code that ‘tricks’ the database into executing unintended commands. The vulnerability occurs primarily because of the features of the SQL language that allow such things as embedding comments using double hyphens (- -), concatenating SQL statements separated by semicolons, and the ability to query metadata from database data dictionaries. The solution to stopping an SQL injection is input validation.

A database management system (DBMS) is a software package designed to define, manipulate, retrieve and manage data in a database. A DBMS generally manipulates the data itself, the data format, field names, record structure and file structure. It also defines rules to validate and manipulate this data. A DBMS relieves users of framing programs for data maintenance. Fourth-generation query languages, such as SQL, are used along with the DBMS package to interact with a database.

A database is the back-end of an application. A DBMS receives instruction from a database administrator (DBA) and accordingly instructs the system to make the necessary changes. These commands can be to load, retrieve or modify existing data from the system.

A DBMS always provides data independence. Any change in storage mechanism and formats are performed without modifying the entire application. (Technopedia Inc., 2017)

Whether you know it or not, databases play an important role in our world today. The history of database management systems goes back a long ways, but the impact on the world as we know it has been an important one

The history of database management systems begins around the time that computers began taking off. In the 1960's, the concept of the database was put in use and also began to grow in commercial use and it was this rise that was an interest to a man named Charles W. Bachman.

It was in 1960 that Bachman came up with the Integrated Database System, the very first DBMS. This got the proverbial ball rolling, as Bachman founded the Database Talk Group along with the group that gave the standardization to the programming language of COBOL. Not to be left out, IBM created their own database system, known IMS, for that of [NASA's Apollo space program](http://www.brighthub.com/science/space/articles/26808.aspx). Both of these are now known as the precursors of navigational databases.

Then in the 1970s, another change was coming. While the above started DBMS, there were in no way easy to use. But then a man named Edgar Codd thought of a way to make things a bit easier. Codd worked for IBM and felt that there had to be a way to make things easier when using these DBMS. He wrote a paper entitled, A Relational Model of Data for Large Shared Data Banks, in which he proposed replacing these current systems with that of tables and rows. This concept would become relational DBMS. And this is where we are today. (Woodard, 2011)

**API – Application Program Interface**

**A**pplication **p**rogram **i**nterface(**API**) is a set of [routines](http://www.webopedia.com/TERM/R/routine.html), [protocols](http://www.webopedia.com/TERM/P/protocol.html), and tools for building [software applications](http://www.webopedia.com/TERM/A/application.html). An API specifies how software components should interact. Additionally, APIs are used when programming graphical user interface ([GUI](http://www.webopedia.com/TERM/G/Graphical_User_Interface_GUI.html)) components. A good API makes it easier to develop a [program](http://www.webopedia.com/TERM/P/program.html) by providing all the building blocks. A [programmer](http://www.webopedia.com/TERM/P/programmer.html) then puts the blocks together.

**TWILIO: Programmable SMS**

When you click "Send SMS", an AJAX request is made that, in turn, triggers a server-side HTTP request to Twilio, which provides a number to SMS, as well as a URL of the photo to be delivered. Image media is automatically transcoded as needed to adapt to carriers and handsets.